Practical-1

AIM: Usage of cables and channels in various types of networks.

Refer these links for better understanding of the same:

1. https://www.wikihow.com/Create-an-Ethernet-Cable
2. https://www.cnet.com/how-to/how-to-make-your-own-ethernet-cable/
3. https://www.ertyu.org/steven_nikkel/ethernetcables.html
4. https://www.youtube.com/watch?v=lullzS740wI&t=148s
5. https://www.youtube.com/watch?v=NmtMPSu--q0
6. **Cabling:** https://www.youtube.com/watch?v=KfhVrivvL7E&list=PLcxPetO_cDzvtZpI-zjKKsc1LZ7K_fDuC&index=14
7. **Crossover cable:** https://www.youtube.com/watch?v=Xc4fWgNDniQ&list=PLcxPetO_cDzvtZpI-zjKKsc1LZ7K_fDuC&index=15
8. **UTP Vs STP:** https://www.youtube.com/watch?v=4cgzuvaukVY&list=PLEWX0h0oWdl0GcSwE3Cs_Uz-EgKVe84Fn

Submission: After writing an answer into this word document, Student needs to change name to his ID followed by practical number. Ex 21ce005_Pr1.docx. Upload on assignment segment. Take the speed as your student ID. Ex. 21ce005, speed would be 5 Mbps.

Rubrics: Nicely drafted document with clarity in answers leads to full marks. Otherwise, submission carries proportional marks.

Refer the following Transmission Modes - Modes of Communication and based on that perform the following case study and write down proper answers of it.

In **Scenario - 1,** as shown in figure 1.1, Let's assume that a car (4-seater Inline) with the constant speed of 60Km/h issues a ticket from the Toll booth to go to its destination. Before the destination there is another Toll Booth which checks the ticket of the car. There is a 120km one way road of 120Km between the two Toll Booths. (Simplex)

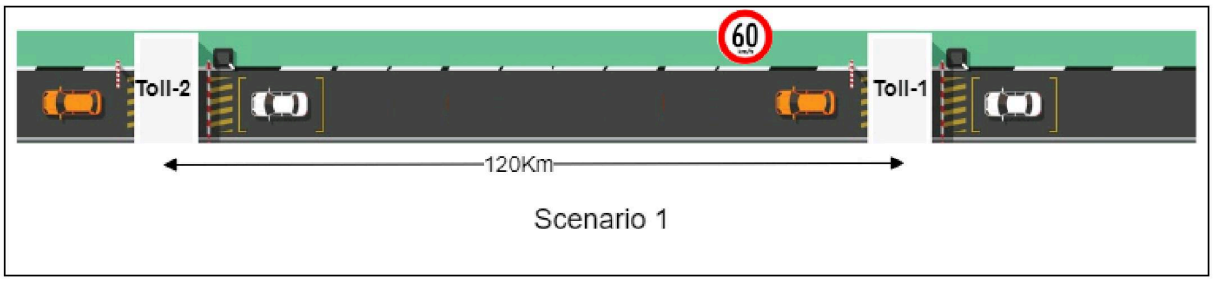


Figure 1.1 Scenario 1

Analogy with computer network

Table 1.2 Simplex Communication

Parameters	Road Transport	Network
Distance	Road Length 120KM	Length of Wire/Channel 120KM
Direction	**One Way** (Either way Both the way)	Simplex**,** Half Duplex Full Duplex
Speed	Car speed 60 km/hr	Link Speed $2.8*10^8$m/s (10 Mbps)
Toll Booth-1	Toll point issue tickets	Transmission Hardware (NIC Card)
Toll Booth-2	Toll point checks tickets	Receiving Hardware (NIC Card)
Time to reach from Toll-1 to Toll-2	2 Hours	428.6 ms
Road	Damar Road	Channel (Signal carries data)
Number of Lane/Road	**Single Lane**	**Single Channel**
Injection	Number of Passengers in Car: 4, they seat back-to-back.	Number of chunks /signals /data
number of deck on car	**Single car**	**Without Multiplexing***

*Multiplexing: combining together

In **Scenario - 2,** as shown in figure 1.2, Let's assume that a car (4-seater Inline) with the constant speed of 60Km/h issues a ticket from the Toll booth to go to its destination. Before the destination there is another Toll Booth which checks the ticket of the car. Both the Stations are connected with a single one-way bridge. (Half Duplex)

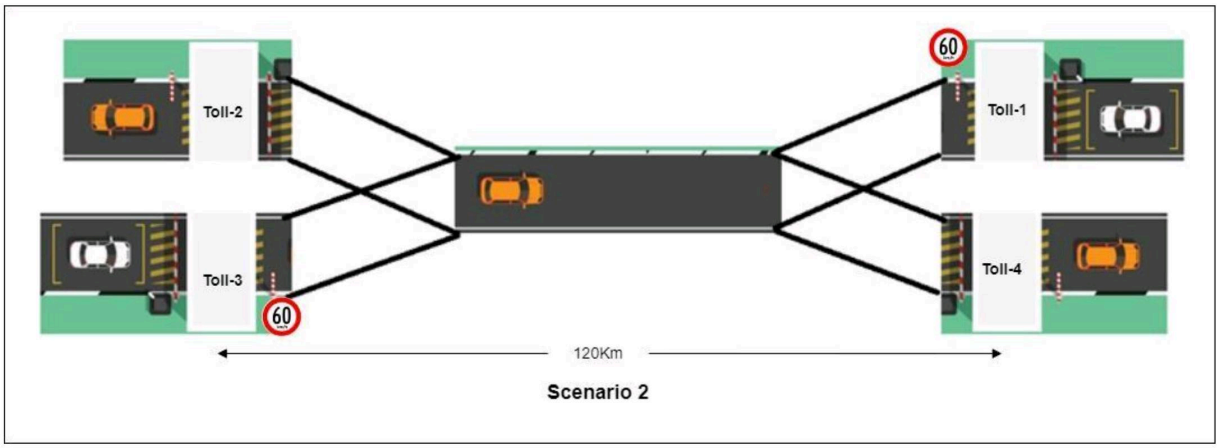


Figure 1.2 Scenario 2

Analogy with computer network: Fill the rows

Table 1.2 Half Duplex Communication

Parameters	Road Transport	Network
Distance	Road Length 120km	Length of Wire/Channel 120KM
Direction	One Way	Simplex, Half Duplex
Speed	Car speed 60 km/hr	Link Speed $2.8*10^8$m/s (10 Mbps)
Toll Booth-1	Toll point issue tickets	Transmission Hardware (NIC Card)
Toll Booth-2	Toll point checks tickets	Receiving Hardware (NIC Card)
Toll Booth-3	Toll point issue tickets	Transmission Hardware (NIC Card)
Toll Booth-4	Toll point checks tickets	Receiving Hardware (NIC Card)
Time to reach from Toll-1 to Toll-2	2 Hours	428.6 ms
Time to reach from Toll-3 to Toll-4	2 Hours	428.6 ms
Road	Damar Road	Channel (Signal carries data)

Width of Lane/Road	3.7 m	-
Number of Lane/Road	Single Lane	Single Channel
Injection	Number of Passengers in Car:4, they seat back-to-back.	Number of chunks /signals /data
Number of deck on car	Single Car	-

In **Scenario - 3,** as shown in figure 1.3, Let's assume that a car (4 seater Inline) with the constant speed of 60Km/h issuing a ticket from the Toll booth to go to its destination. Before the destination there is another Toll Booth which checks the ticket of the car. There is a two way road of 120Km between the two Toll Booths. One road to go from toll-1 to toll-2 and second is to go from toll-3 to toll-4. (Full duplex)

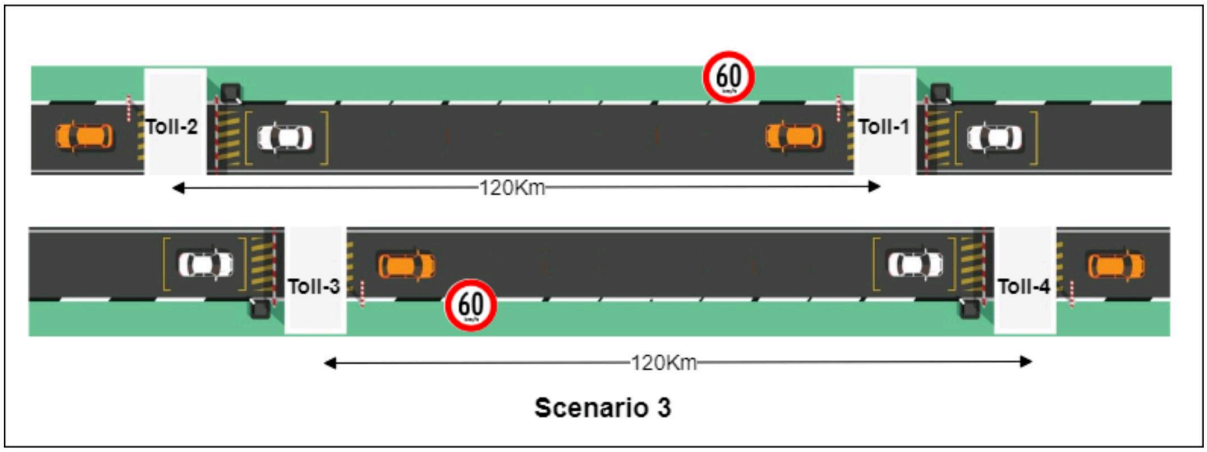


Figure 1.3 Scenario 3

Analogy with computer network: Fill the rows

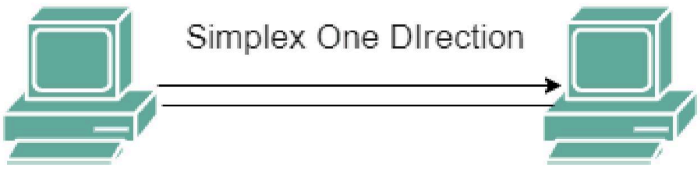
Table 1.3 Full Duplex Communication

Parameters	Road Transport	Network
Distance	Road Length 120km	Length of Wire/Channel 120KM
Direction	Both the Way	Full Duplex
Speed	Car speed 60 km/hr	Link Speed $2.8*10^8$m/s (10 Mbps)

Toll Booth-1	Toll point issue tickets	Transmission Hardware (NIC Card)
Toll Booth-2	Toll point checks tickets	Receiving Hardware (NIC Card)
Toll Booth-3	Toll point issue tickets	Transmission Hardware (NIC Card)
Toll Booth-4	Toll point checks tickets	Receiving Hardware (NIC Card)
Time to reach from Toll-1 to Toll-2	2 Hours	428.6 ms
Time to reach from Toll-3 to Toll-4	2 Hours	428.6 ms
Road	Damar Road	Channel (Signal carries data)
Width of Lane/Road	7.5 m	-
Number of Lane/Road	Multiple Lane	Multiple Channel
Injection	Number of Passengers in Car:4, they seat back-to-back.	Number of chunks /signals /data
Number of deck on car	Single Car	-

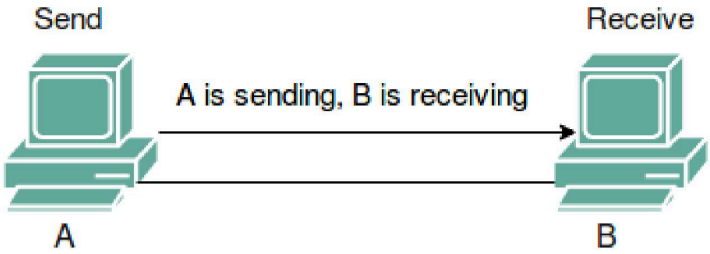
Simplex:

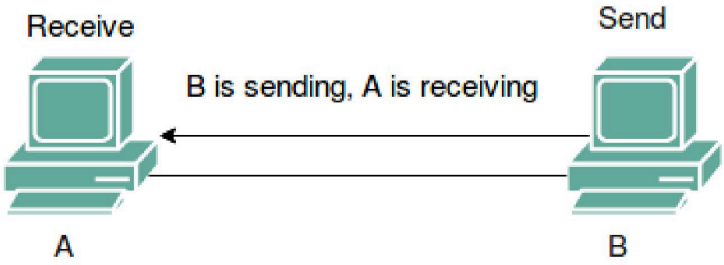
- Simplex channel operation
- one way only
- one person talks and other listens



Half Duplex:

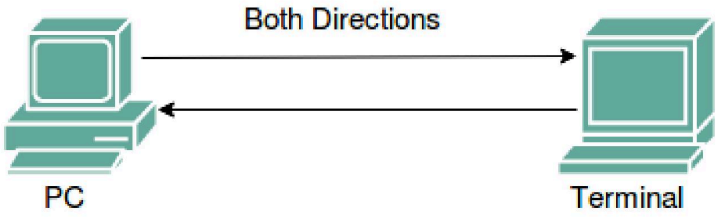
- Two-way communication
- Two people can talk but one at a time





Full Duplex:

- Both ways of communication.
- Two people can talk simultaneously.



Exercise: Calculate the cost of the Network 100 metre network of 2 Machines. Also write a list of equipment required for each type and medium of network.

Table 1.4 Exercise

	Wired	**Wireless**	**Fiber Optic Cable**
Simplex	Requires a transmitter and a receiver. Examples include one-way cable TV transmission.	Requires a transmitter and a receiver. Examples include one-way radio broadcast.	Requires an optical transmitter and an optical receiver.
Half Duplex	Requires devices capable of alternating between transmitting and receiving, such as network interface cards (NICs) supporting half-duplex mode, and network cables.	Requires devices capable of switching between transmitting and receiving, such as wireless routers, access points, and wireless network cards.	Requires devices capable of alternating between transmitting and receiving optical signals, such as transceivers and optical fiber cables.
Full Duplex	Requires devices capable of simultaneous bidirectional communication, such as NICs supporting full-duplex mode, and network cables.	Requires devices and protocols that support simultaneous bidirectional communication, such as Wi-Fi 6 (802.11ax) or newer standards.	Requires devices capable of simultaneous bidirectional communication over optical fiber, such as full-duplex transceivers and optical fiber cables.

Cost Calculation: The cost of the network will vary depending on the specific equipment chosen, brand preferences, and installation requirements. Here are some general cost estimates for the equipment:

1. **Equipment Cost:**
    - Wired: Cost of NICs, network cables, and any additional networking hardware (e.g., switches or hubs).
    - Wireless: Cost of wireless routers, access points, wireless network cards, and any additional hardware (e.g., antennas or repeaters).
    - Optical Fiber: Cost of optical transceivers, optical fiber cables, and any additional equipment (e.g., media converters or switches with fiber ports).
2. **Installation Cost:**
    - Wiring and Cable Installation: Cost of labor for cable installation, termination, and testing.
    - Wireless Network Setup: Cost of configuring wireless routers, access points, and security settings.
    - Optical Fiber Installation: Cost of fiber optic cable installation, splicing, and termination.

In **Scenario - 4,** Let's assume that a car (4-seater Inline) with the constant speed of 60Km/h issues a ticket from the Toll booth to go to its destination. Before the destination there is another Toll Booth which checks the ticket of the car. There are two lane roads to go from Toll-1 to Toll-2 and Toll-3 to Toll-4. By Two roads the capacity of the road increases the number of cars which can travel through. (Full Duplex with Improved bandwidth)

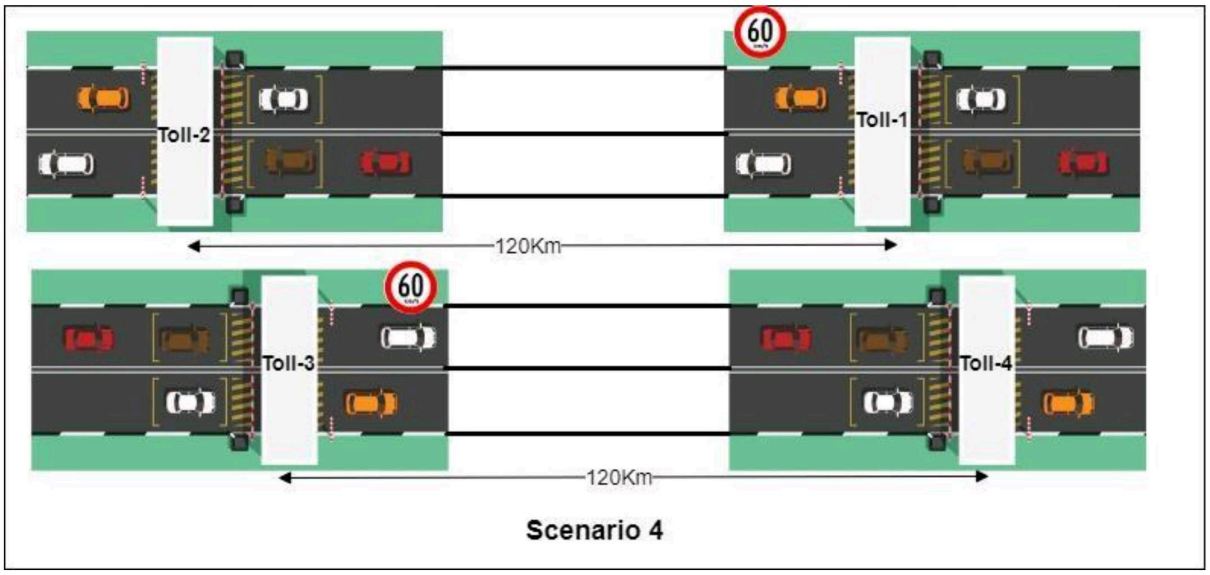


Figure 1.4 Scenario 4

Analogy with computer network

Table 1.5 Full Duplex with Improved bandwidth Communication

Parameters	Road Transport	Network
Distance	Road Length 120km	Length of Wire/Channel 120KM
Direction	Two Way	**Full Duplex** with Improved bandwidth
Speed	Car speed 60 km/hr	Link Speed $2.8*10^8$m/s (10 Mbps)
Toll Booth-1	Toll point issue tickets	Transmission Hardware (NIC Card)
Toll Booth-2	Toll point checks tickets	Receiving Hardware (NIC Card)
Toll Booth-3	Toll point issue tickets	Transmission Hardware (NIC Card)

Toll Booth-4	Toll point checks tickets	Receiving Hardware (NIC Card)
Time to reach from Toll-1 to Toll-2	2 Hours	428.6 ms
Time to reach from Toll-3 to Toll-4	2 Hours	428.6 ms
Road	Damar Road	Channel (Signal carries data)
Width of Lane/Road	15m	-
Number of Lane/Road	Multiple Lane	Multiple Channel
Injection	Number of Passengers in Car:4, they seat back-to-back.	Number of chunks /signals /data
Number of deck on car	**Single car**	With multiplexing

In **Scenario -5**, Let's assume that a Double Decker car (4-seater Inline, 2 floors) with the constant speed of 60Km/h issuing a ticket from Toll booth to go to its destination. Before the destination there is another Toll Booth which checks the ticket of the car. Both the Stations are connected with a single one-way bridge. Only one double decker car can go through. **(Multiplexing)**

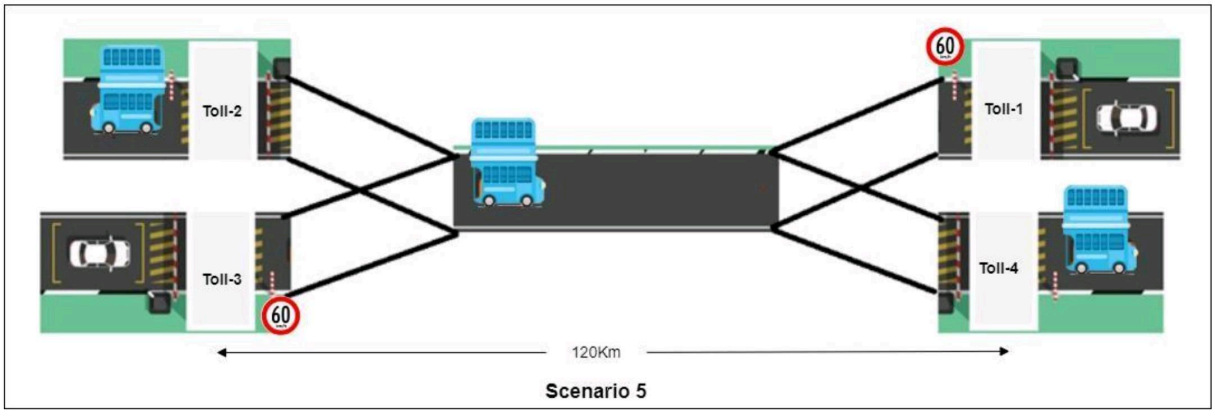


Figure 1.5 Scenario 5

Analogy with computer network: Fill the rows

Table 1.6 Multiplex Communication

Parameters	Road Transport	Network
Distance	Road Length 120km	Length of Wire/Channel 120KM
Direction	One Way	Half Duplex
Speed	Car speed 60 km/hr	Link Speed $2.8*10^8$m/s (10 Mbps)
Toll Booth-1	Toll point issue tickets	Transmission Hardware (NIC Card)
Toll Booth-2	Toll point checks tickets	Receiving Hardware (NIC Card)
Toll Booth-3	Toll point issue tickets	Transmission Hardware (NIC Card)
Toll Booth-4	Toll point checks tickets	Receiving Hardware (NIC Card)
Time to reach from Toll-1 to Toll-2	2 Hours	428.6 ms
Time to reach from Toll-3 to Toll-4	2 Hours	428.6 ms
Road	Damar Road	Channel (Signal carries data)
Width of Lane/Road	3.75m	
Number of Lane/Road	**Single Lane**	**Single Channel**
Injection	Number of Passengers in Car: 4, 2 floors	Number of chunks /signals /data
Number of deck on car	**Double Decker car**	**With Multiplexing**

Scenario 6, as shown in figure 1.6, Let's say we want to travel from Ahmedabad to Surat. In this first we go through Express Highway till Vadodara after that we route for National Highway. Ahmedabad to Vadodara takes less time as cars can speed up to 100Km/h. Vadodara to Surat takes much time as cars can speed only up to 60Km/h. (Data Rate Changes with respect to link speed)

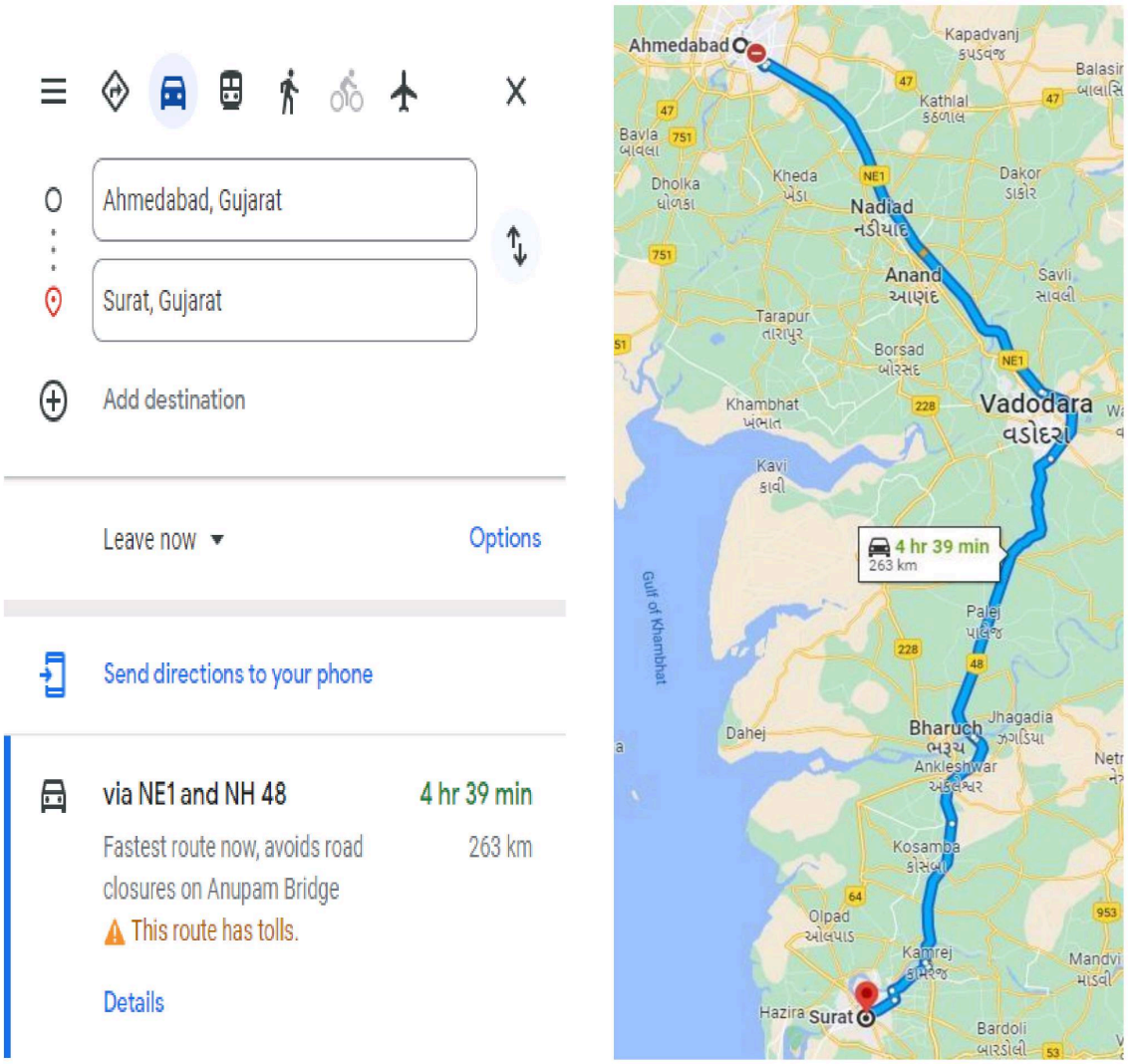


Figure 1.6 Different speed on different type of road

Write conclusion with respect to computer networks:

Ans:

The scenario you've described with the travel from Ahmedabad to Surat using both an Express Highway and a National Highway can be metaphorically related to computer networks in terms of data transfer rates and network performance. Let's draw some conclusions based on this analogy:

1. Express Highway as High-Speed Link:

- The portion of the journey from Ahmedabad to Vadodara on the Express Highway, where cars can speed up to 100 km/h, can be equated to a high-speed link in a computer network.
- In computer networks, high-speed links or connections with greater bandwidth allow for faster data transfer rates. This could be analogous to a network segment with high data rate capabilities, such as a fiber-optic connection or a high-speed wired network.

2. National Highway as Low-Speed Link:
    - The segment from Vadodara to Surat on the National Highway, where cars can only travel at 60 km/h, represents a slower link in the journey.
    - In computer networks, this could be analogous to a network segment with a lower data transfer rate, such as a connection with limited bandwidth or slower wireless connectivity.
3. Data Rate Changes and Link Speed:
    - The scenario highlights a change in data rate as the journey progresses, transitioning from a high-speed link to a lower-speed link.
    - In computer networks, data rate changes can occur between different segments of a network. For instance, within a network, data might move at different speeds depending on the type of connection, the technology used, or the network infrastructure.

Types of Delay:

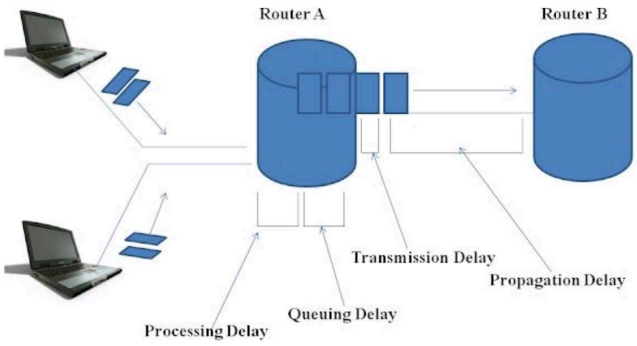


Figure 1.9 Scenario 5

In Scenario -1**,** different cars coming from each direction have to wait for the signal to cross the road as the road is busy because other cars are crossing through the same cross road.

Exercise: Write down transmission delay, queueing delay of computer network with respect to following cross road analogy.

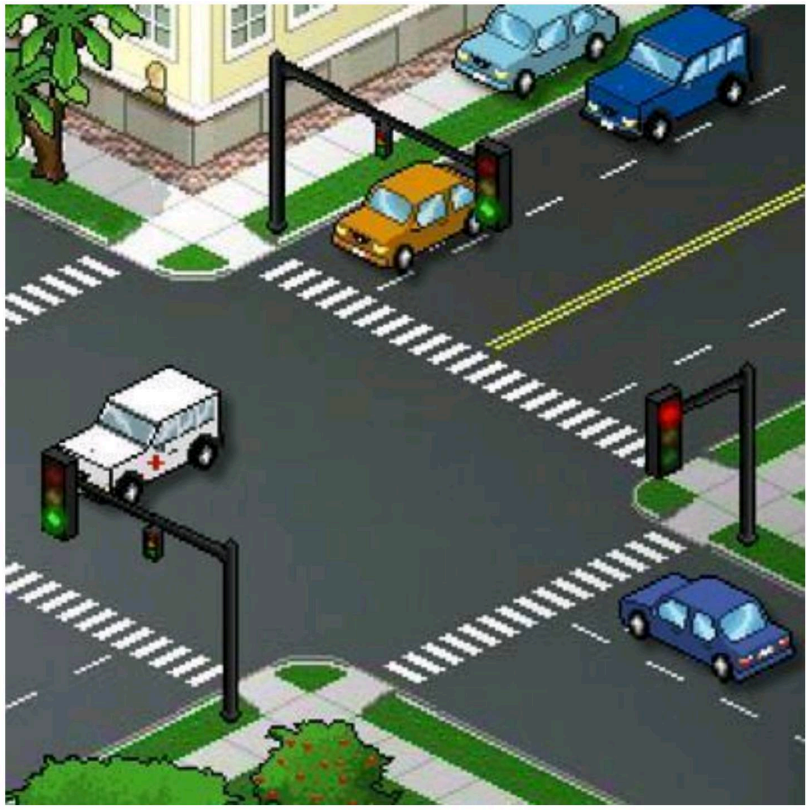


Figure 1.8 Scenario 5

In the crossroad analogy, transmission delay is represented by the time it takes for a car to cross the road after the signal changes, and queueing delay is illustrated by the time cars spend waiting in a queue before being allowed to proceed. These analogies help to visualize and understand the concepts of transmission delay and queueing delay in the context of computer networks.

1. **Propagation Delay:**
    - Propagation delay is the time it takes for a signal to travel from the source to the destination. It is influenced by the physical distance between the sender and receiver and the speed of the medium (such as copper wire, fiber-optic cable, or wireless).
2. **Transmission Delay:**
    - Transmission delay is the time it takes to push all the bits of a packet onto the network medium. It depends on the size of the data packet and the data rate

of the link. The formula for transmission delay is given by Transmission Delay=Packet SizeLink BandwidthTransmission Delay=Link Band widthPacket Size.

3. **Processing Delay:**
    - Processing delay is the time it takes for a router or a host to process the incoming data. This includes tasks such as packet header processing, error checking, and making routing decisions.
4. **Queueing Delay:**
    - Queueing delay occurs when a packet has to wait in a queue before it can be transmitted. This delay is influenced by the congestion level of the network and the queuing algorithms in use.

Case Study:

Refer to the following diagram and identify which mode of communication happens.

1) Refer to the following two scenarios and identify which type of communication is done.

Scenario 1: Can different radio stations work at the same time using the same frequency.

Ans:

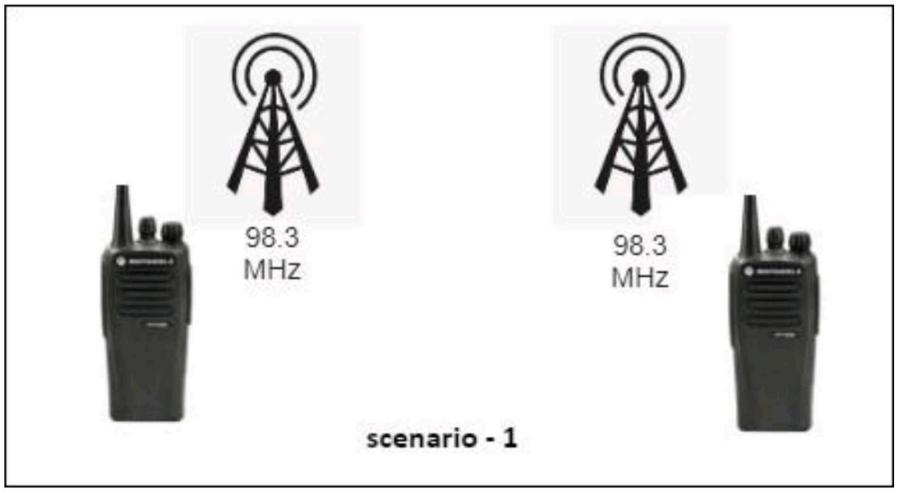


Figure 1.10 Scenario 5

Scenario 2: Can different radio stations work at the same time using different frequencies.

Ans: Yes, different radio stations can work at the same time using different frequencies, and this concept is based on Frequency Division Multiplexing (FDM). FDM is a multiplexing

technique that allows multiple signals to share the same communication channel without interfering with each other by assigning distinct frequency bands to each signal.

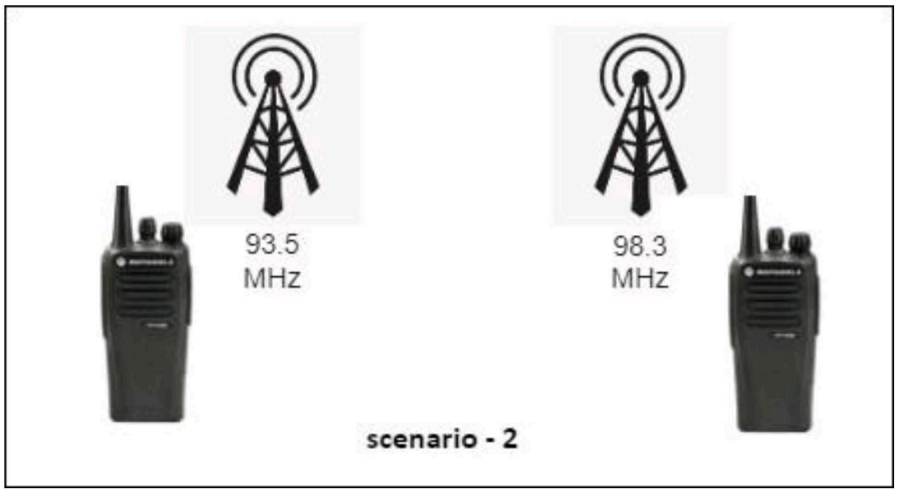


Figure 1.11 Scenario 5

2) Refer to the following diagram and identify which type of communication is done.

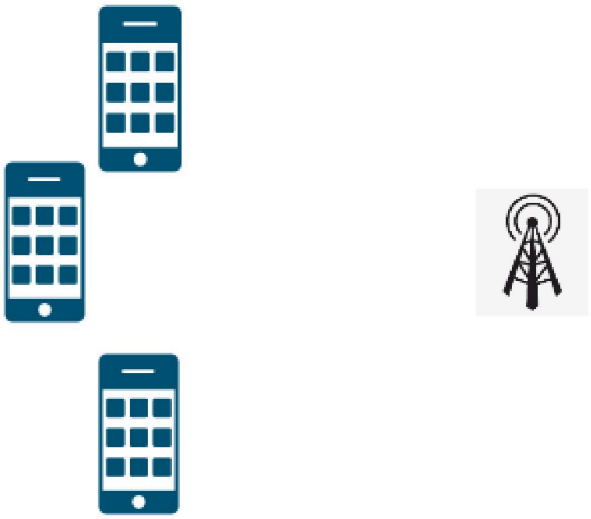


Figure 1.12 Scenario 5

Ans: **Metropolitan Area Network (MAN)**

3) Refer to the following diagram and identify which type of communication is done.

Figure 1.13 Scenario 5

Ans: **Metropolitan Area Network (MAN)**

4) Refer to the following diagram, figure 1.14, and identify which type of communication is done.

Different radio stations in different cities and they are communicating to each other so which type of communication is happen between this radio stations.

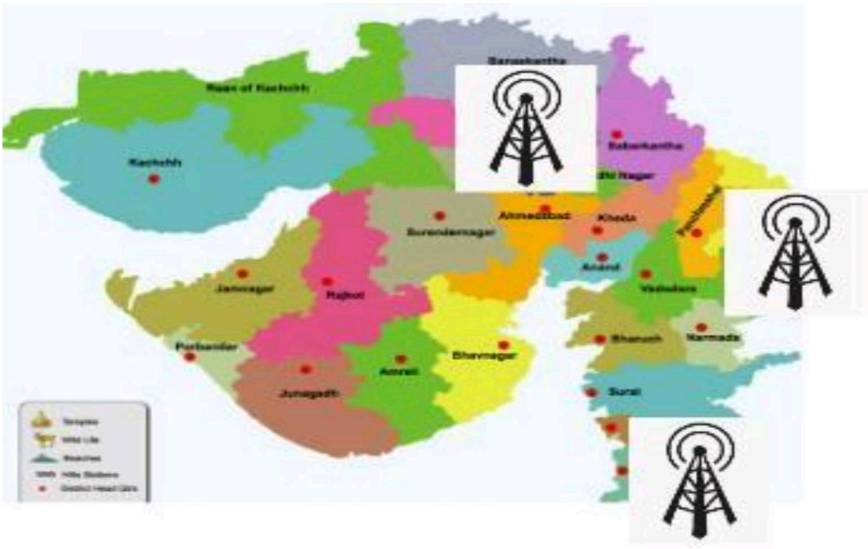


Figure 1.14 Scenario 5

Ans: **Wide Area Network (WAN)**

5) Refer to the following diagram and identify which type of communication is done.

Figure 1.15 Scenario 5

Ans: **Personal Area Network (PAN)**

6) Refer to the following diagram and identify which type of communication is done.

Figure 1.16 Scenario 5

Ans: **Wide Area Network (WAN)**

Study the different types of Cables in Networking and based on that perform the following case study.

Refer to the following link.

https://fcit.usf.edu/network/chap4/chap4.htm

When it comes to connecting the networks, we can connect them in two different ways

1. Wired Connection
2. Wireless connection

Different types of Networking Cables:

1. Unshielded Twisted Pair (UTP) Cable
2. Shielded Twisted Pair (STP) Cable
3. Coaxial Cable
4. Fiber Optic Cable
5. Cable Installation Guides
6. Wireless LANs
7. Unshielded Twisted Pair (UTP) Cable

Case Study:

1) Refer to the following Linear Bus Topology and make the connection using appropriate cables.

Link: https://fcit.usf.edu/network/chap5/chap5.htm

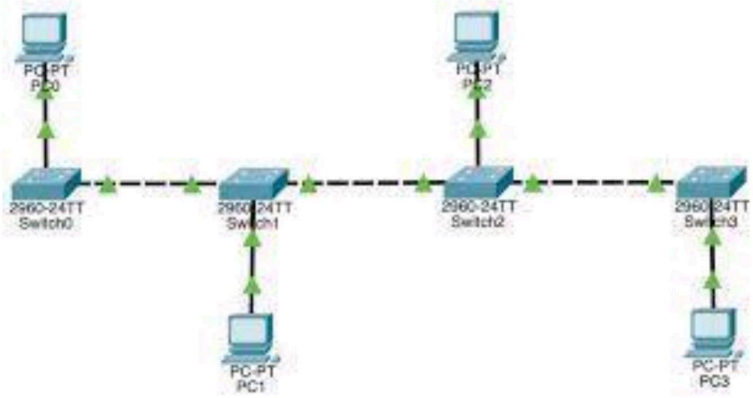


Figure 1.17 Scenario 5

2) Refer to the following Star Topology and make the connection using appropriate cables.

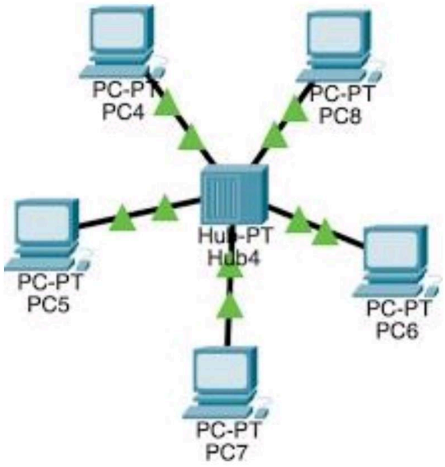


Figure 1.18 Scenario 5

3) Refer to the following Tree Topology and make the connection using appropriate cables.

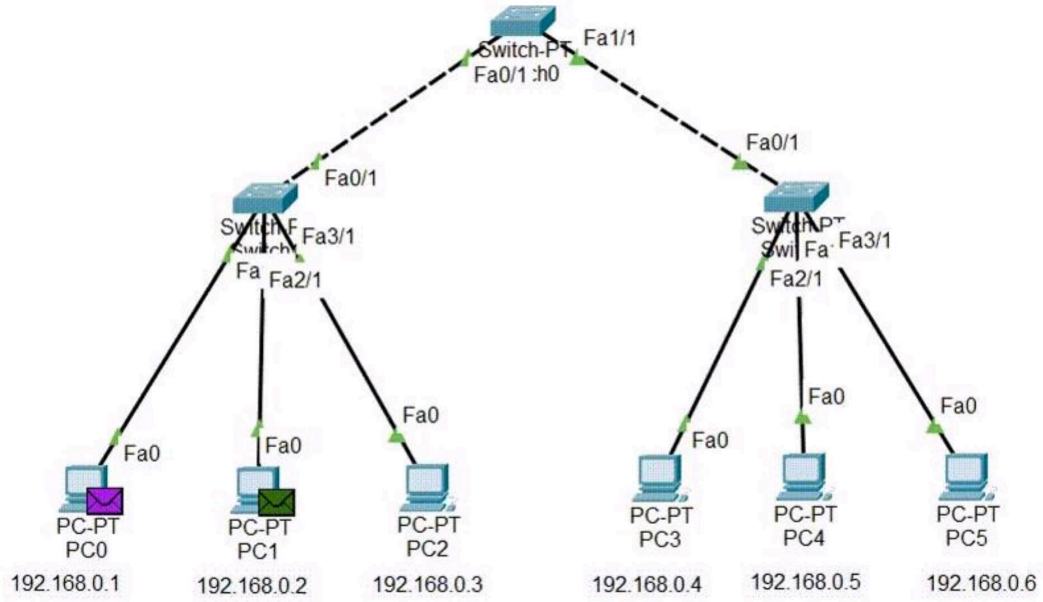


Figure 1.19 Scenario 5

Refer to the following Network Diagram - Typical Simple Home Network

https://fcit.usf.edu/network/chap4/chap4.htm

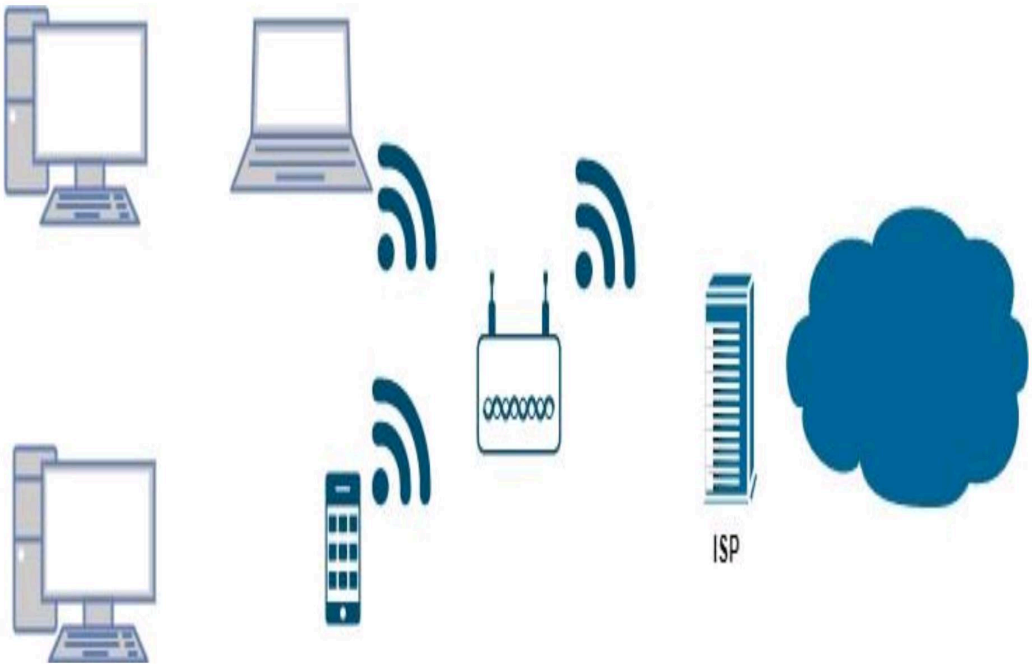


Figure 1.20 Scenario 5

Refer to the following images and based on that let's understand the concept of Multiplexing and Demultiplexing.

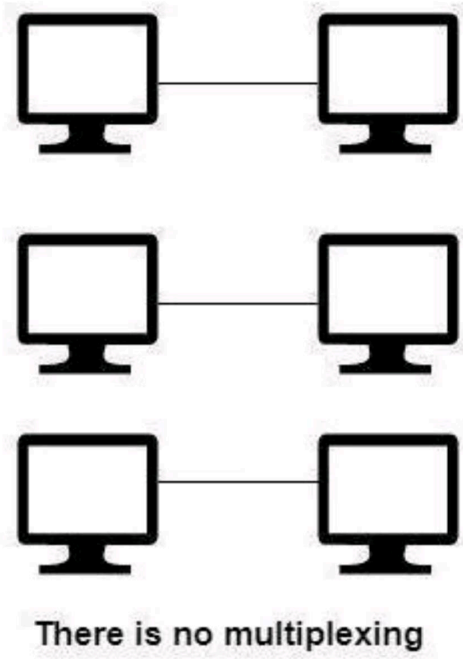


Figure 1.21 Scenario 5

In above point to point topology, all the nodes can send and receive data but with their own channels. so required three own channels.

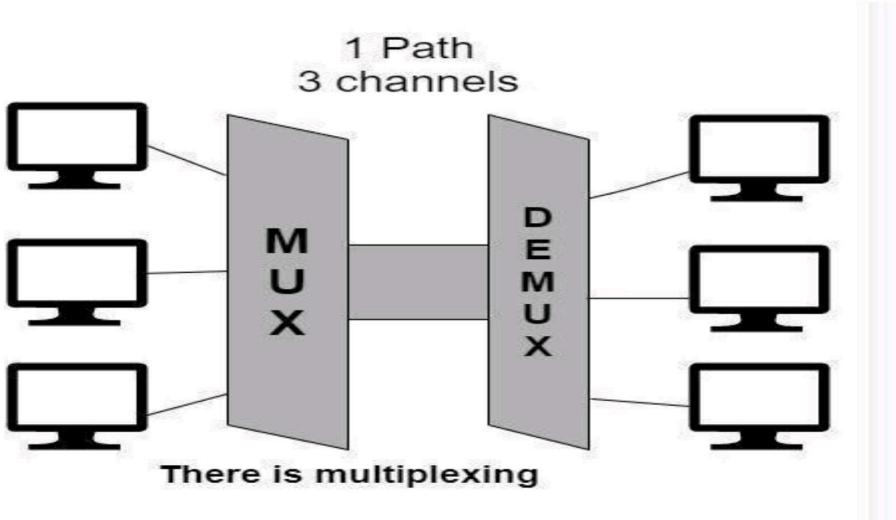


Figure 1.22 Scenario 5

In the above diagram, With the help of multiplexing, more than one signal can be sent easily over a single medium or link. Multiplexing helps in the effective utilization of the bandwidth of the medium.

Questions

Students are advised to give answers to following questions after going through in-depth study of all above references:

1. What is the significance of Braided Shield in Shielded Twisted Pair (STP) cable?

Answer: the significance of the braided shield in Shielded Twisted Pair (STP) cables includes:

1. Protection against electromagnetic interference (EMI) and radio frequency interference (RFI).
2. Grounding to dissipate induced electrical charges.
3. Mechanical protection for internal components.
4. Flexibility for versatile installation and usage.

2. List down various network cables in markets other than UTP and STP.

Answer: Various types of network cables available in the market other than UTP and STP:

1. Coaxial Cable (Coax)
2. Fiber Optic Cable
3. Twisted Pair Cable Categories (e.g., Cat6a, Cat7)
4. Power over Ethernet (PoE) Cable
5. Plenum Cable
6. Direct Burial Cable
7. Ethernet Crossover Cable

3. Where UTP and STP cables are used?

Answer:

1. UTP (Unshielded Twisted Pair) Cables:

- Used extensively in Ethernet networks, including LAN (Local Area Network) environments such as offices, homes, and schools.
- Commonly employed for telephone lines, broadband internet connections, and home networking applications.
- Preferred choice for short to medium distance data transmissions due to its cost-effectiveness and ease of installation.

2.STP (Shielded Twisted Pair) Cables:

- Employed in environments with higher levels of electromagnetic interference (EMI), such as industrial settings, manufacturing plants, and areas with electrical machinery.
- Utilized in environments where data integrity and reliability are critical, such as data centers, server rooms, and high-security installations.
- Offers superior protection against EMI and RFI (Radio Frequency Interference), making it suitable for applications where signal integrity is paramount.

4. List down the four parameters, on which the UTP cables are categorised.
Answer: Unshielded Twisted Pair (UTP) cables are categorized based on the following four parameters:

1. **Category (Cat):**
    - Indicates the performance specifications of the cable, including data transmission speed and bandwidth capacity. Common categories include Cat5e, Cat6, Cat6a, and Cat7.
2. **Bandwidth:**
    - Refers to the maximum frequency range over which the cable can transmit data. Higher bandwidth cables support faster data transmission rates and can handle larger amounts of data.
3. **Frequency:**
    - Specifies the frequency range over which the cable is tested for performance. Higher frequencies correspond to higher data transmission speeds.
4. **Twists per Inch (TPI):**
    - Indicates the number of twists in the cable's twisted pairs per inch of cable length. A higher TPI value typically results in better noise immunity and signal quality.

5. What is the difference in pin architecture of Cross-over cable and straight through cable?
Answer: the main difference in pin architecture between a crossover cable and a straight-through cable is the arrangement of wires at the connectors:

1. **Straight-Through Cable:**
    - Both ends of the cable have the same pin configuration, meaning that the wires are connected straight through from one end to the other.
    - In Ethernet cables, the pinouts are typically aligned such that the transmit (TX) pins on one end connect to the receive (RX) pins on the other end.
2. **Crossover Cable:**
    - The pin configuration at one end of the cable is reversed compared to the other end.

- In Ethernet cables, this means that the transmit (TX) pins on one end connect to the transmit (TX) pins on the other end, and the receive (RX) pins connect to the receive (RX) pins. This configuration allows for direct communication between similar devices without the need for a network switch or hub.

6. Why is twisted pair used in network cable?
Answer: twisted pair cables are used in network cables because:

1. **Reduced Electromagnetic Interference (EMI):**
    - Twisting the pairs of wires helps cancel out electromagnetic interference (EMI) from external sources, such as power lines or electronic devices, resulting in clearer transmission signals.
2. **Minimized Crosstalk:**
    - Twisting the pairs also reduces crosstalk, which is interference caused by adjacent wire pairs in the cable. This ensures that data signals remain distinct and do not interfere with each other.
3. **Cost-Effectiveness:**
    - Twisted pair cables are relatively inexpensive to manufacture, making them a cost-effective choice for networking applications.
4. **Versatility:**
    - Twisted pair cables can support various data transmission speeds and are suitable for both short and long-distance connections, making them versatile for different network environments.

7. Why do we require two wires for signal transmission in cable and one wire in optic transmission in fibre optic?
Answer: the difference in the number of wires required for signal transmission between cable (such as twisted pair) and fiber optic transmission is due to the nature of the mediums:

1. **Cable (Twisted Pair):**
    - In cable transmission, such as twisted pair cables, two wires are used for signal transmission because electrical signals require a complete circuit to flow. One wire carries the signal (transmit), and the other acts as a reference (ground or return path), completing the circuit.
2. **Fiber Optic Transmission:**
    - In fiber optic transmission, only one wire (fiber optic strand) is needed because data is transmitted using light signals instead of electrical signals. The light travels through the core of the fiber optic strand, and there is no need for a return path as in electrical transmission. Therefore, only one strand is required for bidirectional communication, allowing for simpler and more efficient transmission.

8. Write down in 2nd column (which cable to use) below:

Connection Scenario	**Cable Type (Cross Over or straight Through)**
Computer to Computer	crossover Ethernet cable
Cable modem to Router	straight-through Ethernet cable
Computer to Cable modem	straight-through Ethernet cable
Computer to Switch	straight-through Ethernet cable
Computer to Hub	straight-through Ethernet cable

9. What is the full form of RJ-45?

Answer: Registered Jack-45

10. List down various RJ connectors with their usage.

Answer: Here's a list of various RJ connectors with their common usage:

1. **RJ-11:**
    - Commonly used for telephone and analog modem connections.
2. **RJ-45:**
    - Used for Ethernet networking connections, including Cat5e, Cat6, and Cat6a cables.
3. **RJ-12:**
    - Similar to RJ-11 but with additional pins. Used for telephone and some data communications.
4. **RJ-48:**
    - Used for T1 and ISDN connections, often found in telecom and networking equipment.
5. **RJ-14:**
    - A combination of RJ-11 and RJ-12, typically used for two-line telephone connections.

11. What signal is used for wireline, wireless and fibre communication? Give example how data is transmitted in simplex, half-duplex and full duplex communication with respect to above cables.

Answer: In wireline, wireless, and fiber communication, different signals are used for data transmission:

1. **Wireline Communication:**
    - Signal: Electrical signals are commonly used for wireline communication.
    - Example: Ethernet cables (UTP or STP) use electrical signals for data transmission.
2. **Wireless Communication:**
    - Signal: Electromagnetic waves, such as radio frequencies or microwaves, are used for wireless communication.
    - Example: Wi-Fi routers transmit data using radio frequency signals.
3. **Fiber Communication:**
    - Signal: Light signals (optical signals) are used for fiber communication.
    - Example: Fiber optic cables transmit data using light signals through the fiber optic strands.

Now, let's look at how data is transmitted in simplex, half-duplex, and full-duplex communication with respect to the above cables:

- **Simplex Communication:**
    - Simplex communication involves one-way data transmission.
    - Example: In a simplex communication scenario, data flows only in one direction. For instance, a sensor sending data to a central monitoring system over a fiber optic cable in a one-way manner.
- **Half-Duplex Communication:**
    - Half-duplex communication allows data transmission in both directions, but not simultaneously.
    - Example: In a half-duplex communication scenario, devices take turns sending and receiving data. For example, two-way radio communication or walkie-talkies operate in half-duplex mode.
- **Full-Duplex Communication:**
    - Full-duplex communication enables simultaneous two-way data transmission.

- Example: In a full-duplex communication scenario, data can be transmitted and received simultaneously. For instance, Ethernet connections using twisted pair cables (UTP/STP) or fiber optic cables support full-duplex communication, allowing devices to transmit and receive data at the same time, enhancing communication efficiency.

12. What are tools used to make network cable with CAT-6 cable? Also write its usage.

Answer: Tools used to make network cables with CAT-6 cable include:

1. **Cable Crimper:**
    - Usage: Used to attach RJ-45 connectors to the ends of CAT-6 cables.
2. **Cable Tester:**
    - Usage: Used to verify the integrity and functionality of the completed CAT-6 cable connections.

These tools are essential for properly terminating CAT-6 cables and ensuring reliable network connections.

13. Mention the companies who are making the cables.

Answer:

14. What is delay and loss in the network?

Answer:

1. **Delay (Latency):**
    - Time taken for data to travel from source to destination.
    - Types include transmission, propagation, processing, and queuing delays.
    - High delays can slow down network performance and response times.
2. **Loss (Packet Loss):**
    - Occurs when packets fail to reach their destination.
    - Reasons include congestion and transmission errors.
    - Can degrade network quality, leading to retransmissions and performance issues.

15. How long does a 10Mbps channel take to transmit 1 bit ?

To calculate the time taken to transmit 1 bit on a 10 Mbps channel, you can use the formula:

Time=1/Data Rate

where:

- Time is the time taken to transmit 1 bit,
- Data Rate is the channel's speed in bits per second (bps).

Using this formula:

Time=1/10 Mbps=110×106 bits/secondTime=10 Mbps1=10×106 bits/second1

Time=1×10−7 secondsTime=1×10−7 seconds

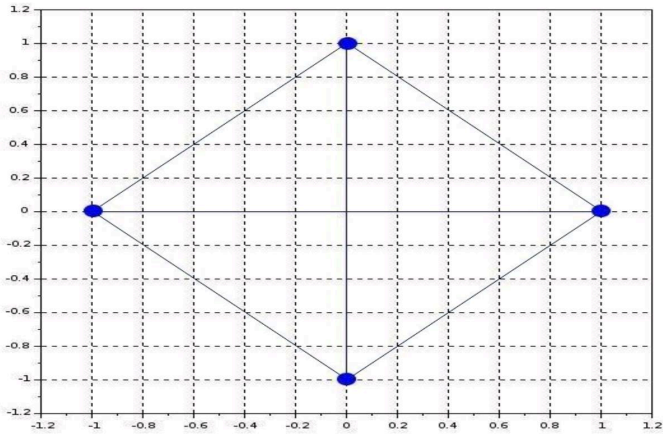
So, it takes 1×10−71×10−7 seconds to transmit 1 bit on a 10 Mbps channel.

16. Mention the companies who are making the following specific cables.

Name of the Cables	**Companies who are making the cables.**
Unshielded Twisted Pair (UTP) Cable	CommScope , Belden ,Panduit ,Siemon , Nexans
Shielded Twisted Pair (STP) Cable	CommScope, Belden , Panduit , Siemon ,Nexans
Coaxial Cable	CommScope, Belden ,Times Microwave Systems , Amphenol ,L-com
Fiber Optic Cable	Corning Incorporated ,Prysmian Group ,CommScope ,OFS (Furukawa Electric) ,AFL Telecommunications

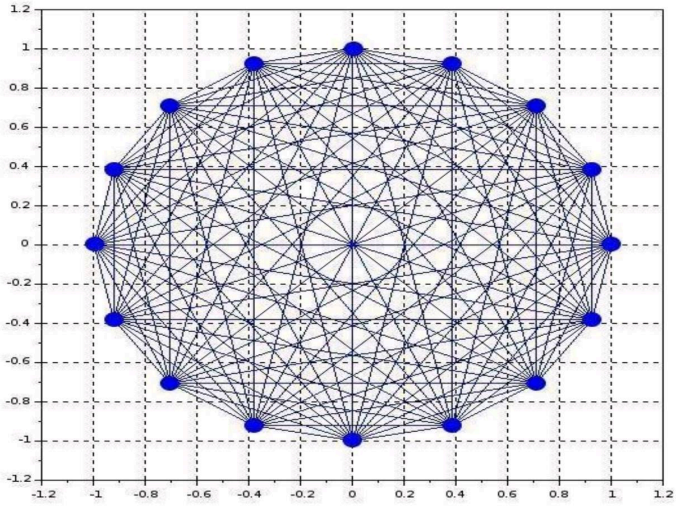
Gate Question:

1. **Calculate the number of cables used for 4 Nodes in mesh topology ?**



Ans : 6

2. **Calculate the number of cables used for 16 Nodes in mesh topology ?**



Ans: 120

3. **In a fully-connected mesh network with 10 computers, a total _____ number of cables are required and _____ number of ports are required for each device. [UGC-NET | UGC NET CS 2016 July]**

A) 40,9

B) 45,10

C) 45,9

D) 50,10

4. **Determine the maximum length of the cable (in km) for transmitting data at a rate of 500 Mbps in an Ethernet LAN with frames of size 10,000 bits. Assume the signal speed in the cable to be 2,00,000 km/s. [GATE | GATE CS 2013]**
   A) 1
   B) 2
   C) 2.5
   D) 5

5. **Consider a source computer transmitting a file of size 10^6 bits to a destination computer (D) over a network of two routers (R1 and R2) and three links (L1, L2 and L3). L1 connects to S to R1; L2 connects to R1 to R2; and L3 connects to R2 to D. Let each link be of length 100 km. Assume signals travel over each link at a speed of 10^8 meters per second. Assume that the link bandwidth on each link is 1Mbps. Let the file be broken down into 1000 packets each of size 1000 bits. Find the total sum of transmission and propagation delays in transmitting the file from S to D?**
   1) 1005 ms
   2) 1010 ms
   3) 3000 ms
   4) 3003 ms

6. **Let us consider a statistical time division multiplexing of packets. The number of sources is 10. In a time unit, a source transmits a packet of 1000 bits. The number of sources sending data for the first 20 time units is 6, 9, 3, 7, 2, 2, 2, 3, 4, 6, 1, 10, 7, 5, 8, 3, 6, 2, 9, 5 respectively. The output capacity of multiplexer is 5000 bits per time unit. Then the average number of backlogged of packets per time unit during the given period is**
   A) 5
   B) 4.45
   C) 3.45
   D) 0

7. **A broadcast channel has 10 nodes and total capacity of 10 Mbps. It uses polling for medium access. Once a node finishes transmission, there is a polling delay of 80 µs to poll the next node. Whenever a node is polled, it is allowed to transmit a maximum of 1000 bytes. The maximum throughput of the broadcast channel is:**
   A) 1 Mbps
   B) 100/11 Mbps
   C) 10 Mbps
   D) 100 Mbps

8. Consider a CSMA/CD network that transmits data at a rate of 100 Mbps (108 bits per second) over a 1 km (kilometre) cable with no repeaters. If the minimum frame size required for this network is 1250 bytes, What is the signal speed (km/sec) in the cable?

1) 8000
2) 10000
3) 16000
4) 20000

9. A network has a data transmission bandwidth of 20 × 106 bits per second. It uses CSMA/CD in the MAC layer. The maximum signal propagation time from one node to another node is 40 microseconds. The minimum size of a frame in the network is 3200 bytes.

10. Which of the following statements is TRUE about CSMA/CD:

A) IEEE 802.11 wireless LAN runs CSMA/CD protocol
B) Ethernet is not based on CSMA/CD protocol
C) CSMA/CD is not suitable for a high propagation delay network like satellite network

11A A network with CSMA/CD protocol in the MAC layer is running at 1Gbps over a 1km cable with no repeaters. The signal speed in the cable is 2 × 108m/sec . The minimum frame size for this network should be:

A) 10000bits
B) 10000bytes
C) 5000 bits
D) 5000bytes

12. Determine the maximum length of the cable (in km) for transmitting data at a rate of 500 Mbps in an Ethernet LAN with frames of size 10, 000 bits. Assume the signal speed in the cable to be 2, 00, 000 km/s.

A) 1
B) 2
C) 2.5
D) 5

13. In an Ethernet local area network, which one of the following statements is TRUE?

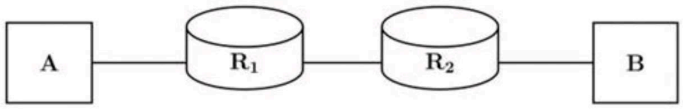
A) A station stops to sense the channel once it starts transmitting a frame.
B) The purpose of the jamming signal is to pad the frames that are smaller than the minimum frame size.
C) A station continues to transmit the packet even after the collision is detected.

D) The exponential back off mechanism reduces the probability of collision on retransmissions.

14. **Consider two hosts X and Y , connected by a single direct link of rate 106 bits/sec. The distance between the two hosts is 10, 000 km and the propagation speed along the link is 2 × 108 m/sec . Host X sends a file of 50, 000 bytes as one large message to host Y continuously. Let the transmission and propagation delays be p milliseconds and q milliseconds respectively. Then the value of p and q are**

A) p = 50 and q = 100
B) p = 50 and q = 400
C) p = 100 and q = 50
D) p = 400 and q = 50

15. **Consider the store and forward packet switched network given below. Assume that the bandwidth of each link is 106 bytes /sec. A user on host A sends a file of size 103 bytes to host B through routers R1 and R2 in three different ways. In the first case a single packet containing the complete file is transmitted from A to B. In the second case, the file is split into 10 equal parts, and these packets are transmitted from A to B. In the third case, the file is split into 20 equal parts and these packets are sent from A to B. Each packet contains 100 bytes of header information along with the user data. Consider only transmission time and ignore processing, queuing and propagation delays. Also assume that there are no errors during transmission. Let T 1, T 2 and T 3 be the times taken to transmit the file in the first, second and third case respectively. Which one of the following is CORRECT?**



A) T 1 < T 2 < T 3
B) T 1 > T 2 > T 3
C) T 2 = T 3, T 3 < T 1
D) T 1 = T 3, T 3 > T 2

16. **Two hosts are connected via a packet switch with 107 bits per second links. Each link has a propagation delay of 20 microseconds. The switch begins forwarding a packet 35 microseconds after it receives the same. If 10000 bits of data are to be transmitted between the two hosts using a packet size of 5000 bits, the time elapsed between the transmission of the first bit of data and the reception of the last bit of the data in microseconds is 145.**

17. Frames of 1000 bits are sent over a 106 bps duplex link between two hosts. The propagation time is 25 ms. Frames are to be transmitted into this link to maximally pack them in transit (within the link).
What is the minimum number of bits (I) that will be required to represent the sequence numbers distinctly? Assume that no time gap needs to be given between transmission of two frames.

A) I = 2
B) I = 3
C) I = 4
D) I = 5

18A A channel has a bit rate of 4 kbps and one-way propagation delay of 20 ms. The channel uses stop and wait protocol. The transmission time of the acknowledgment frame is negligible. To get a channel efficiency of at least 50%, the minimum frame size should be

A) 80 bytes
B) 80 bits
C) 160 bytes
D) 160 bits

Practical-2

AIM: Understand and identify header fields of layers of TCP/IP protocol stack.

Tools Required: WordPad or Notepad.
Submission: After writing the answer into this word document, Student needs to change name to his ID followed by a practical number. Ex 20ce005_Pr1.docx. Upload on assignment segment.
Rubrics: Nicely drafted document with clarity in answers leads to full marks. Otherwise, submission carries a proportional mark.

Watch and refer following videos for a better understanding of the header fields of layers of TCP/IP:

Material 1.	**Ethernet frame ():** https://www.youtube.com/watch?v=SoTRqDLND6Y
Material 2.	**IPv4 header format ()**: https://www.youtube.com/watch?v=3Y70y6dM7Cs
Material 3.	**IPv4 Vs IPv6()**: https://www.youtube.com/watch?v=NkE9_iRPi1I
Material 4.	**TCP and UDP ():** https://www.youtube.com/watch?v=r4HbLQuqvrM

Students need to fill the empty table and write answers to questions.

As per the discussion in classroom, any user starts internet access through browser or network applications. Following figure 2.1 explain scenario of receiving data at NIC Card. NIC card receives signals and it converts into sequence of 0's and 1's. After receiving data it sends data for the further processing to TCP/IP protocol stack. In this exercise you need to identify boundaries of fields of headers, describe and understand flow of information in protocol stack.

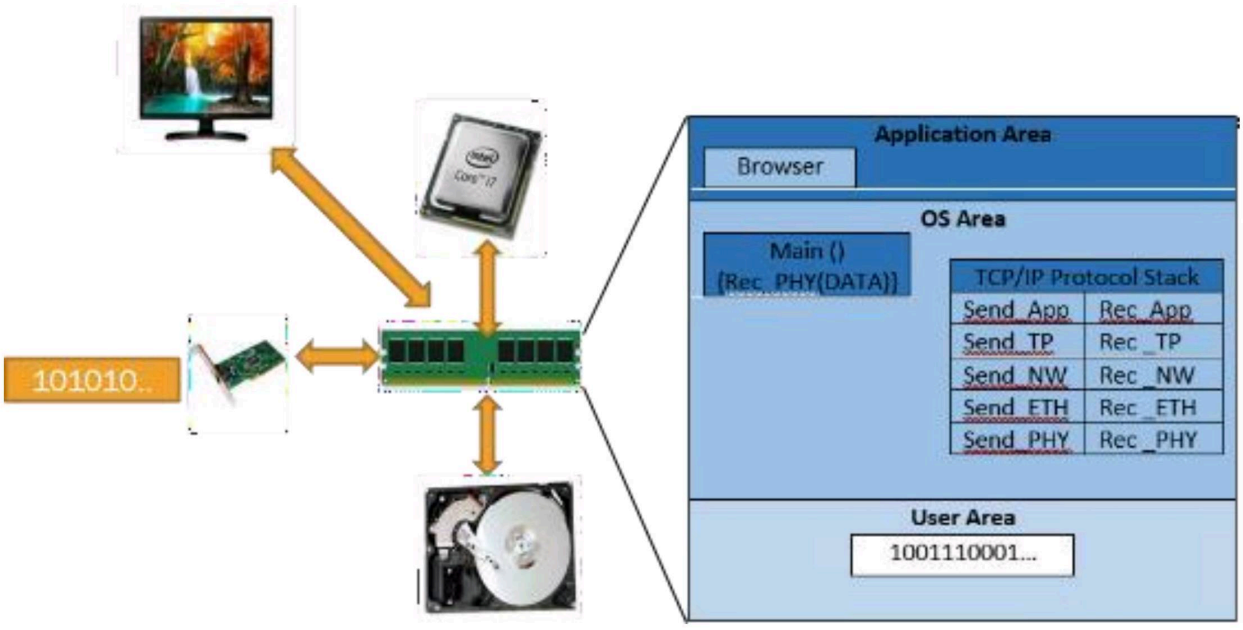


Figure 2.1 Real Scenario

2.1 Input data stream: TCP

This is the data stream which receiver NIC card receives from wire and stores into memory. Length of bits stream is 432 bits.

000000000001101010001100011010111011010101100111010001101100011010001010001101111001111110001000010000000000001000101000000000000000000010100000010101101111010100000000000000100000000000001100000000000000000010101100000100000000110001111011000111011111010101101110100111011000101011100110000000011011101101001001111011110111100100000100000011010001001110101000000010000000100000000101011111110111011100000000000000000

Abstract view of data with respect to the location of headers and data in the actual data stream.

Data Link (Ethernet) Header	Network Header	Transport Header	Data

Initial 112 bits contains Ethernet Header (Refer section 2.2), Next 160 bits contains IP Header (Refer section 2.3), Next 160 bits contains TCP Header (Refer section 2.4).

2.2 Header format of Ethernet

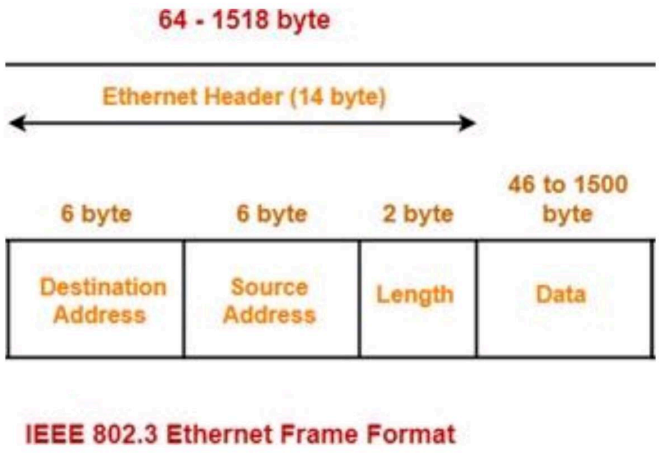


Figure 2.2 Ethernet Header Format

Section 2.1 contains bit stream. copy and paste respected number of bits into following table 2.1 to prepare ethernet header field boundary.

Table 2.1 Header format of ethernet

000000000001101010001100011010110111 0111011010101100	1110100011011000110100010100011 01111001111110001	0000100000 000000

From table 2.1, fill table 2.2 with respected value and explanation meaning of each field. Refer the following link for better understanding. Refer video 1 in material 1 for further understanding.

Reference Link : https://en.wikipedia.org/wiki/Ethernet_frame#Header
https://en.wikipedia.org/wiki/EtherType

Table 2.2 Header fields of Ethernet

Header Field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
Destination MAC Address	48 bits	00:1A:8C:6B:76:AC	Receiver's MAC address
Source MAC Address	48 bits	E8:D8:D1:46:F3F1	Sender's MAC address
Type	16 bits	0x800	0x800 indicates, Network Header type is IPv4 Header

2.3 Header format of Network

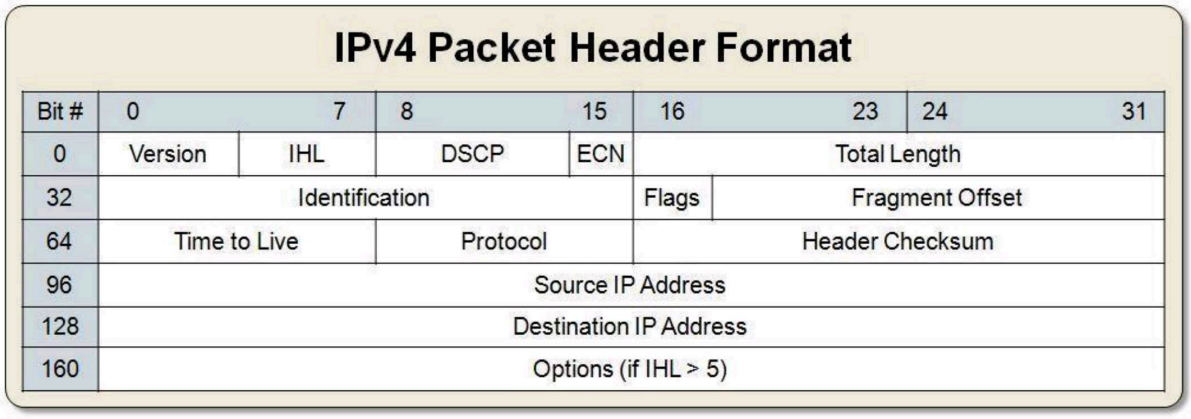


Figure 2.3 IPv4 header format

Section 2.1 contains bit stream. copy and paste respected number of bits into following table 2.3 to prepare ethernet header field boundary.

Table 2.3 Header format of network

0100	0101	000000	00	0000000000101000
0001010110111101			010	0000000000000
10000000		00000110		0000000000000000
10101100000100000000110001111011				
10001110111110101011011101001110				

From table 2.3, fill table 2.4 with respected value and explanation meaning of each field. Refer the following link for better understanding. Refer video 2 in material 2 for further understanding.

Reference Links:

https://en.wikipedia.org/wiki/IPv4#Header

DCSP & ECN: https://en.wikipedia.org/wiki/Type_of_service#DSCP_and_ECN

Flags: https://en.wikipedia.org/wiki/IPv4#Flags

Protocol: https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers

Table 2.4 Header fields of Network

Header Field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
Version	4 bits	0x4	IP Datagram version 4
IHL	4 bites	0x5	5*32bits=160bits=20bytes
DSCP	6 bits	0x0	---
ECN	2 bits	0x0	---
Total length	16 bits	0x28	Total length of 40 bytes
Identification	16 bits	0x15BD	
flags	3 bits	0x2	2 bit More Fragment (MF)
Fragment offset	13 bits	0x0	This packet does not contain fragments.
Time to live	8 bits	0x80	128 Hops / Routers
Protocol	8 bits	0x06	This packet should be give to TCP receive procedure. As its value indicates TCP.
Header checksum	16 bits	0x0	No checksum included in this header.
Source IP Address	32 bits	172.16.12.123	Source IP: 172.16.12.123, its local machine
Destination IP Address	32 bits	142.250.183.78	Destination: 142.250.183.78, it is situated in_____country

2.4 Header format of transport layer: TCP

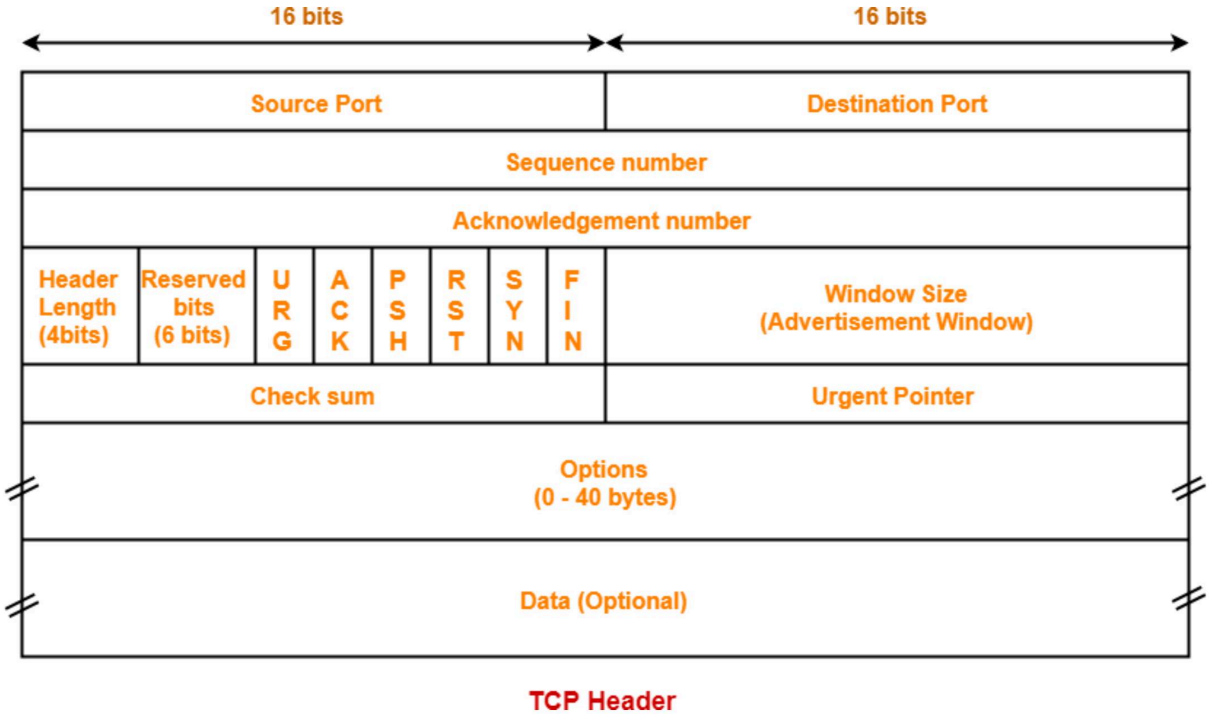


Figure 2.4 TCP Header format

Section 2.1 contains bit stream. copy and paste respected number of bits into following table 2.5 to prepare ethernet header field boundary.

Table 2.5 Header fields of transport layer

1100010101110011								0000000110111011
01001001111011110111110100011010								
11110010000010000001101000100111								
0101	000000	0	1	0	0	0	0	0001000000001010
1111111011101110								0000000000000000

From table 2.5, fill table 2.6 with respected value and explanation meaning of each field. Refer the following link for better understanding. Refer video 4 in material 4 for further understanding.

Reference Link :
https://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_segment_structure
Flags: https://www.gatevidyalay.com/transmission-control-protocol-tcp-header/
Port : https://www.adminsub.net/tcp-udp-port-finder/

Table 2.6 Header fields of Transport Layer: _____

Header Field Name	**Length of Field (in bits)**	**Header field Value (Hex Value)**	**Meaning**
Source Port	16 Bits	50547	Sender machine's application's logical port number 50547.
Destination Port	16 Bits	443	Receiver machine's receiving logical port number 443 which indicates source wants communicate security using https protocol.
Sequence Number	32 Bits	0x49EF7D1A	Unique ID assigned by sender to maintain order of packers at receiver side.
Acknowledgement Number	32 Bits	0xF2081A27	This is acknowledge of sent packet.
Header Length	4 Bits	0x5	Total header Length is 5*32bits=160bits=20bytes
Reserved Bits	6 Bits	0x0	-
URG	1 Bit	0	
ACK	1 Bit	1	This packet contains valid acknowledgement number.
PSH	1 Bit	0	No Push
RST	1 Bit	0	No RST
SYN	1 Bit	0	No SYN
FIN	1 Bit	0	NO Fin
Window Size	16 Bits	0x100A	4106
Checksum	16 Bits	0xFEEE	Error identification in packet.
Urgent Pointer	16 Bits	0x0	No urgent content in this packet.

Exercise-1: Input Sequence TCP

11101000110110001101000101000110111100111111000100000000000110101000110001101011
01110110101011000000100000000000010001010000000000000000001010001011111111010010
01000000000000000100000000000011011001110110100000110011100111011100011000110011
10101100000100000000110001111011000000011011101111110010110010000011000100010000
00000101111000001110010000000000010000101001101001010000000100000000000011111011
10110000100111010000000000000000000000000000000000000000000000000000000000000000

Header fields of Ethernet

Header Field Name	**Length of Field (in bits)**	**Header field Value (Hex Value)**	**Meaning**
Destination MAC Address	48 bits	E8:D8:D1:46:F3:F1	Receiver's MAC address
Source MAC Address	48 bits	00:1A:8C:6B:76:AC	Senders MAC address
Type	16 bits	800	0x800 indicates, Network Header type isIPv4 Header

Header fields of Network

Header Field Name	**Length of Field (in bits)**	**Header field Value (Hex Value)**	**Meaning**
VERSION	4bit	4	IP Datagram version 4
IHL	4bit	5	5*32bits=160bits=20bytes
DSCP	6bit	0	----------
ECN	2bit	0	----------
TOTAL LENGHT	16bit	28	Total length of 40 bytes
IDENTIFICATION	16bit	BFD2	
FLAGS	3bit	2	2 bit More Fragment (MF)
FRAGMENT OFFSET	13bit	0	-------
TIME TO LIVE	8bit	40	
PROTOCOL	8bit	6	This packet should be given to TCP receive procedure. As its value indicates TCP.
HEADER CHECK SUM	16bit	CED0	
SOURCE IP ADDRESS	32bit	673B8C66	259.89.320.258
DESTINATION ADDRESS	32bit	AC100C7B	172.16.12.123

Header fields of Transport Layer: _____

Header Field Name	**Length of Field (in bits)**	**Header field Value (Hex Value)**	**Meaning**
Source Port	16 Bits	01BB	Sender machine's application's logical port number 01BB.
Destination Port	16 Bits	F2C8	Receiver machine's receiving logical port number F2C8 which indicates source wants communicate security using https protocol.
Sequence Number	32 Bits	311005E0	Unique ID assigned by sender to maintain order of packers at receiver side.
Acknowledgement Number	32 Bits	E400429A	This is acknowledge of sent packet.
Header Length	4 Bits	0x5	Total header Length is 5*32bits=160bits=20bytes
Reserved Bits	6 Bits	0x0	-
URG	1 Bit	0	
ACK	1 Bit	1	This packet contains valid acknowledgement number.
PSH	1 Bit	0	No Push
RST	1 Bit	0	No RST
SYN	1 Bit	0	No SYN
FIN	1 Bit	0	NO Fin
Window Size	16 Bits	0xFB	4106
Checksum	16 Bits	B09D	Error identification in packet.
Urgent Pointer	16 Bits	0x0	No urgent content in this packet.

Exercise-2: Input Sequence of UDP

11101000110110001101000101000110111100111111000100000000010100000101011010101011
11110010011001110000100000000000010001010000000000000000001010000010000101011001
00000000000000001000000000010001101010011000100110101100000100000000101101000111
10101100000100000000110001111011111001110010000000001101001111010000000000010100
10001101001111111111010010000000000001011110011100000100000000000000000000000100
00000000000000010000111111011001000000000000000000000000000000000000000000000000

Header fields of Ethernet

Header Field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
Destination MAC Address	48 bits	E8:D8:D1:46:F3:F1	Receiver's MAC address
Source MAC Address	48bits	50:56:AB:F2:67	Sender's MAC address
Type	16bits	0x800	800 indicates IPV4

Header fields of Network

Header Field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
VERSION	4	4	IP Datagram version 4
IHL	4	5	5*32bits=160bits=20bytes
DSCP	6	0	----------
ECN	2	0	----------
TOTAL LENGHT	16	28	Total length of 40 bytes
IDENTIFICATION	16	2159	
FLAGS	3	0	2 bit More Fragment (MF)
FRAGMENT OFFSET	13	0	-------
TIME TO LIVE	8	80	
PROTOCOL	8	11	This packet should be give to TCP receive procedure. As its value indicates TCP.
HEADER CHECK SUM	16	A989	
SOURCE IP ADDRESS	32	AC100B47	172.16.11.71
DESTINATION ADDRESS	32	AC100C7B	172.16.12.123

Header fields of Transport Layer: _____

Header Field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
Destination MAC Address	48	E7200D3D0014	Receiver's MAC address
Source MAC Address	48	8D3FF48005E7	Sender's MAC address
Type	16	400	

Exercise-3: Input Sequence: ARP Broadcast

111111111111111111111111111111111111111111111111000000110001111011010010100
011100010100010000001000000001100000000000000001000010000000000000000011000000100
000000000000000111100000011000111101101001010100011100010100010010101100000010000
000010000001000010000000000000000000000000000000000000000000000000001010110000010000
000001111001110100000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000

Header fields of Ethernet

Header Field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
Destination MAC Address	48 bits	FFFFFFFFFFFF	Receiver's MAC address
Source MAC Address	48 bits	E063DA5471 4 4	Sender's MAC address
Type	16bits	806	

Header fields of __________________

Header field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
VERSION	4	0	------
IHL	4	0	-------
DSCP	6	0	------
ECN	2	1	
TOTAL LENGHT	16	800	
IDENTIFICATIO N	16	604	
FLAGS	3	0	-------
FRAGMENT OFFSET	13	1	
TIME TO LIVE	8	E0	
PROTOCOL	8	63	
HEADER CHECK SUM	16	DA54	
SOURCE IP ADDRESS	32	7144AC10	113.68.172.16
DESTINATION ADDRESS	32	8210000	8.33.0.0

Exercise-4: Input Sequence: ARP Reply

11111111111111111111111111111111111111111111111010011000001000110111111100111011
11110011100010110000100000000110000000000000000100001000000000000000011000000100
00000000000000100100110000010001101111110011101111100111000101110101100000100000
00001110011010110000000000000000000000000000000000000000000000001010110000010000
00001110011010110000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000

Header fields of Ethernet

Header Field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
Destination MAC Address	48 bits	FFFFFFFFFFFF	Receiver's MAC address
Source MAC Address	48 bits	4C11BF9DF38B	Sender's MAC address
Type	16bits	806	

Header fields of _____

Header Field Name	Length of Field (in bits)	Header field Value (Hex Value)	Meaning
VERSION	4	0	------
IHL	4	0	------
DSCP	6	0	------
ECN	2	1	
TOTAL LENGHT	16	800	
IDENTIFICATION	16	604	
FLAGS	3	0	------
FRAGMENT OFFSET	13	2	
TIME TO LIVE	8	4C	
PROTOCOL	8	11	
HEADER CHECK SUM	16	BF9D	
SOURCE IP ADDRESS	32	F38BAC10	243.139.172.16
DESTINATION ADDRESS	32	E6B0000	14.107.0.0

Questions and answers:

1. What do you mean by TTL (Time to Live)?

Answer: TTL (Time to Live) in networking refers to a value in IP packets that dictates the maximum time or number of hops a packet can traverse in a network before being discarded.

2. What is the significance of Sequence Number and Acknowledgment Number in TCP format?

Answer: The sequence number in TCP format is essential for ordering and reconstructing data packets, while the acknowledgment number confirms the receipt of data and facilitates reliable data transmission between sender and receiver.

3. What is the full form of the MAC address? What is the significance of source and destination MAC address?

Answer: The full form of MAC address is Media Access Control address, and the source MAC address identifies the sender of a network packet while the destination MAC address specifies the intended recipient, crucial for data forwarding at the data link layer.

4. What is the full form of IP, TCP, UDP and ARP?

Answer: IP: Internet Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
ARP: Address Resolution Protocol

Gate Questions:

1. **What is the maximum size of data that the application layer can pass on to the TCP layer below?**
   A) Any size
   B) 216 bytes - size of TCP header
   C) 216 bytes
   D) 1500 bytes

2. **The protocol data unit (PDU) for the application layer in the Internet stack is:**
   A) Segment
   B) Datagram
   C) Message
   D) Frame

3. **A TCP message consisting of 2100 bytes is passed to IP for delivery across two networks. The first network can carry a maximum payload of 1200 bytes per frame and the second network can carry a maximum payload of 400 bytes per frame, excluding network overhead. Assume that IP overhead per packet is 20 bytes. What is the total IP overhead in the second network for this transmission?**
   A) 40 bytes
   B) 80 bytes
   C) 120 bytes
   D) 160 bytes

4. **Which one of the following statements is FALSE?**
   A) TCP guarantees a minimum communication rate
   B) TCP ensures in-order delivery
   C) TCP reacts to congestion by reducing sender window size
   D) TCP employs retransmission to compensate for packet loss

5. **In TCP, a unique sequence number is assigned to each**
   A) byte
   B) word
   C) segment
   D) message

6. **Consider the following statements about the timeout value used in TCP.**
   i. **The timeout value is set to the RTT (Round Trip Time) measured during TCP connection establishment for the entire duration of the connection.**
   ii. **Appropriate RTT estimation algorithm is used to set the timeout value of a TCP connection.**
   iii. **Timeout value is set to twice the propagation delay from the sender to the receiver.**

   Which of the following choices hold?
   A) (i) is false, but (ii) and (iii) are true
   B) (i) and (iii) are false, but (ii) is true
   C) (i) and (ii) are false, but (iii) is true
   D) (i), (ii) and (iii) are false

7. **Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header ans 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0.**
   The fragmentation offset value stored in the third fragment is_____.
   Note –This was ..Numerical Type question.
   A) 0
   B) 72
   C) 144
   D) 216

8. **Consider two hosts P and Q connected through a router R. The maximum transfer unit (MTU) value of the link between P and R is 1500 bytes, and between R and Q is 820 bytes.**

   A TCP segment of size 1400 bytes was transferred from P to Q through R, with IP identification value as 0×1234. Assume that the IP header size is 20 bytes. Further, the packet is allowed to be fragmented, i.e., Don't Fragment (DF) flag in the IP header is not set by P.

   Which of the following statements is/are correct?
   A) Two fragments are created at R and the IP datagram size carrying the second fragment is 620 bytes.
   B) If the second fragment is lost, R will resend the fragment with the IP identification value 0×1234.
   C) If the second fragment is lost, P is required to resend the whole TCP segment.
   D) TCP destination port can be determined by analysing only the second fragment.

9. **One of the header fields in an IP datagram is the Time to Live(TTL)field.Which of the following statements best explains the need for this field?**
   A) It can be used to prioritize packets
   B) It can be used to reduce delays
   C) It can be used to optimize throughput
   D) It can be used to prevent packet looping

10. **In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are:**
    A) Last fragment, 2400 and 2789
    B) First fragment, 2400 and 2759
    C) Last fragment, 2400 and 2759
    D) Middle fragment, 300 and 689

11. **The maximum number of IPv4 router addresses that can be listed in the record route (RR) option field of an IPv4 header is 9.**

12. **Consider an IP packet with a length of 4, 500 bytes that includes a 20 – byte IPv4 header ans 40 - byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the**

outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0.

The fragmentation offset value stored in the third fragment is 119.

13. **For which one of the following reasons does internet protocol(IP) use the time-to-live(TTL) field in IP datagram header?**
    A) Ensure packets reach destination within that time
    B) Discard packets that reach later than that time
    C) Prevent packets from looping indefinitely
    D) Limit the time for which a packet gets queued in intermediate routers

14. **One of the header fields in an IP datagram is the Time-to-Live (TTL) field. Which of the following statements best explains the need for this field?**
    A) It can be used to prioritize packets.
    B) It can be used to reduce delays.
    C) It can be used to optimize throughput.
    D) It can be used to prevent packet looping.

15. **Host A (on TCP/IP v4 network A) sends an IP datagram D to host B (also on TCP/IP v4 network B). Assume that no error occurred during the transmission of D. When D reaches B, which of the following IP header field(s) may be different from that of the original datagram D?**
    i. TTL
    ii. Checksum
    iii. Fragment Offset
    A) i only
    B) i and ii only
    C) ii and iii only
    D) i, ii and iii

16. **Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?**
    A) 6 and 925
    B) 6 and 7400
    C) 7 and 1110
    D) 7 and 8880

17. **An IP datagram of size 1000 bytes arrives at a router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes . Assume that the size of the IP header is 20 bytes .**

    The number of fragments that the IP datagram will be divided into for transmission is 11.

18. **In the TCP/IP protocol suite, which one of the following is NOT part of the IP header?**
    A) Fragment Offset

B) Source IP address
C) Destination IP address
D) Destination port number

Practical-3

AIM: Allocating IP address to network topologies

Student should be able to apply IP addresses to

1. Topology: two directly connected computers
2. Topology: four computers connected by switches
3. Topology: two networks connected by Router

Various networking commands:

- ping
- ipconfig
- arp –a
- netstat
- netbios
- tracert
- hostname
- nmap

Reference Videos

1. Refer Video(25 minutes) of practical-4
2. IP address: https://www.youtube.com/watch?v=ykz4oUPWACw
3. IP address assignment in Video: https://www.youtube.com/watch?v=vcAtxgDsl00

Reference for commands:

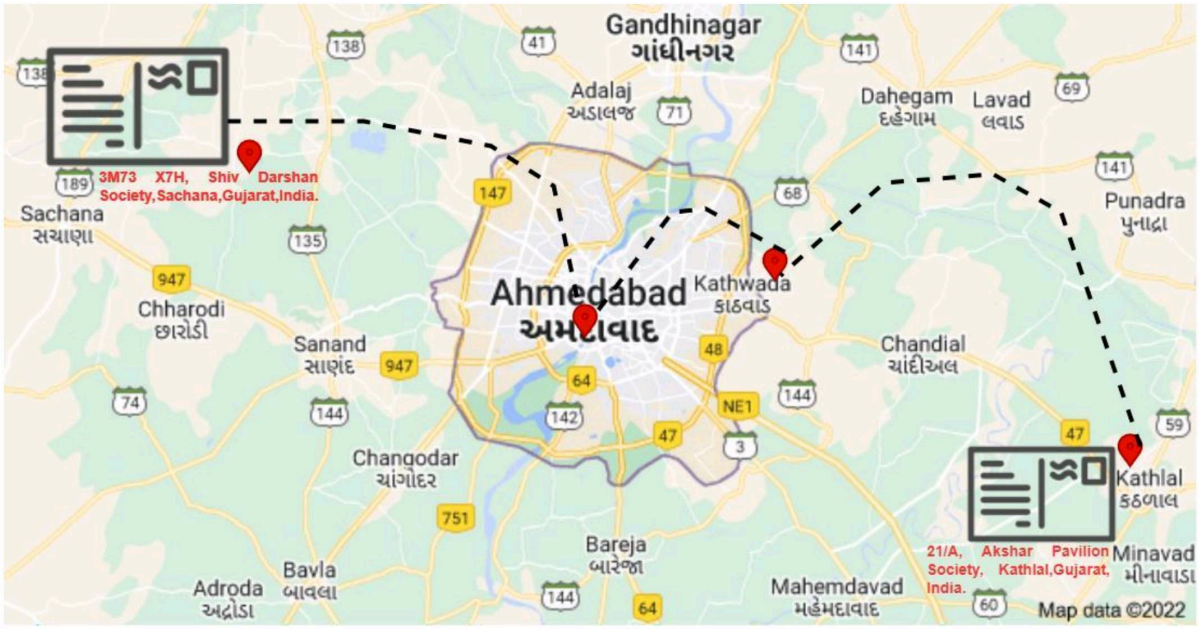
1. https://lizardsystems.com/articles/network-command-line-utilities/
2. https://www.youtube.com/watch?v=nH85pddWWAk
3. https://www.youtube.com/watch?v=rurs7cdT5cc&t=7s

Note: While applying IP address, student needs to allocate IP address as per his/her student ID. For Example, if student ID is 20ce005 then IP address allocation for the first network should start with 5.0.0.0. For subsequent networks, it should start with ID+1 i.e. 6.0.0.0, 7.0.0.0 and so on.

Submission: After writing an answer into this word document, Student needs to change name to his ID followed by practical number. Ex 20ce005_Pr1.docx. Upload on assignment segment.
Rubrics: Nicely drafted document with clarity in answers leads to full marks. Otherwise, submission carries proportional marks.
Recommended to type, avoid copy-paste to increase your typing skill.

Refer to the following scenarios and let's understand What is an IP Address and Purpose of IP Address.

Scenario : 1

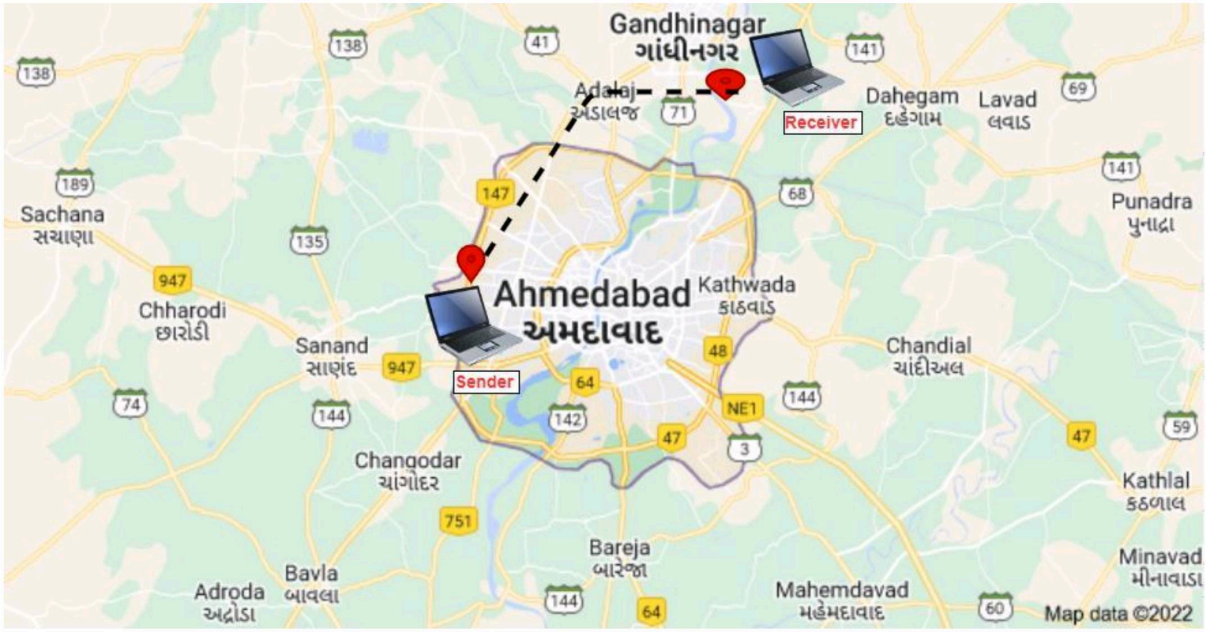


In this first scenario, an envelope is sent from sachana to kathlal. But there was some check point like ahmedabad, kathwada and then the envelope is delivered to kathlal.

Justify the following statement.

1. Was there any difficulty faced during sending the envelope from sender to receiver ?

Scenario : 2

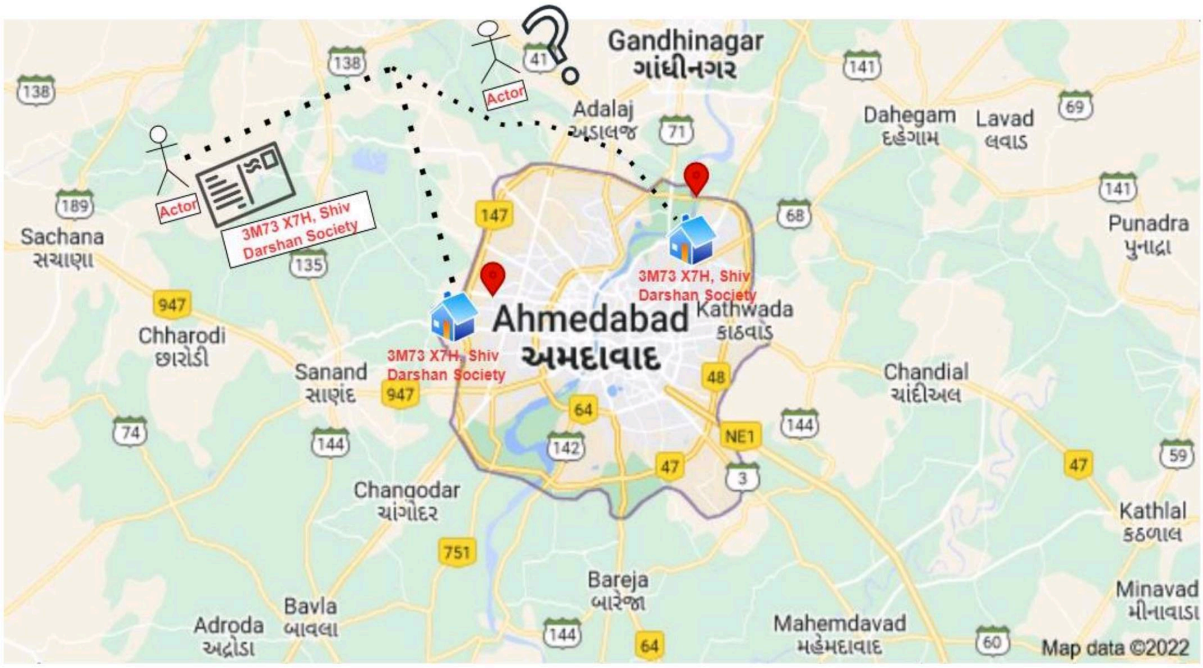


In this second scenario, the sender was located at Ahmedabad and wanted to send a file to the receiver who was located at Gandhinagar. But at the time of sending a file to the receiver, the receiver's machine was powered off. So, can the receiver receive the file from the sender or not?

Justify the following statement.

2. Was there any difficulty faced during sending the file from sender to receiver? If yes then what would be the solution for it.

Scenario: 3

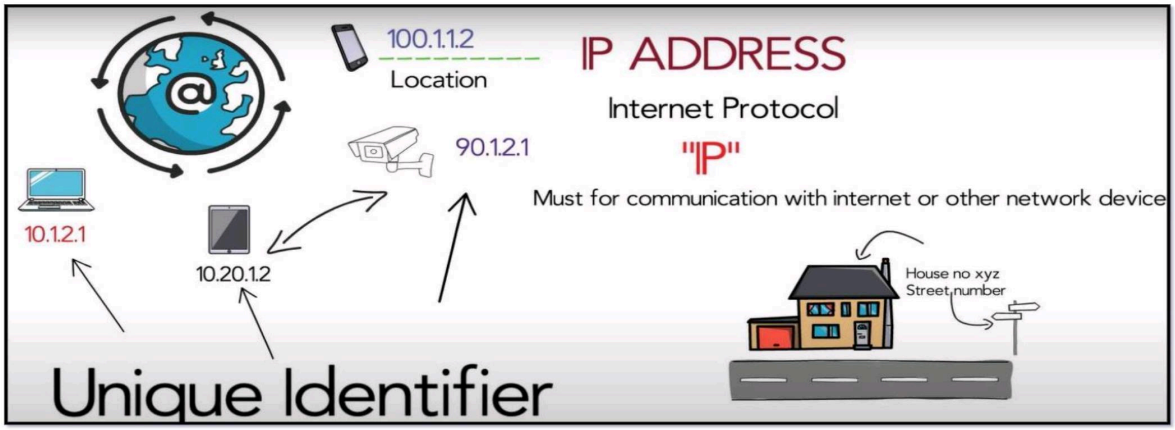


Refer the above image, and justify your answer

Question:

Can the envelope be sent to the proper destination?

Scenario: 4



An IP address also acts like a return address on postal mail. When a letter you've mailed is delivered to the wrong address, you get the letter back if you include a return address on the envelope. The same holds true for email. When you write to an invalid recipient (such as someone who left their job and no longer has a company email address) your IP address lets the company's mail server send you back a bounce message so that you know your email wasn't sent to the right place.

From the above all scenarios, what would be the conclusion?

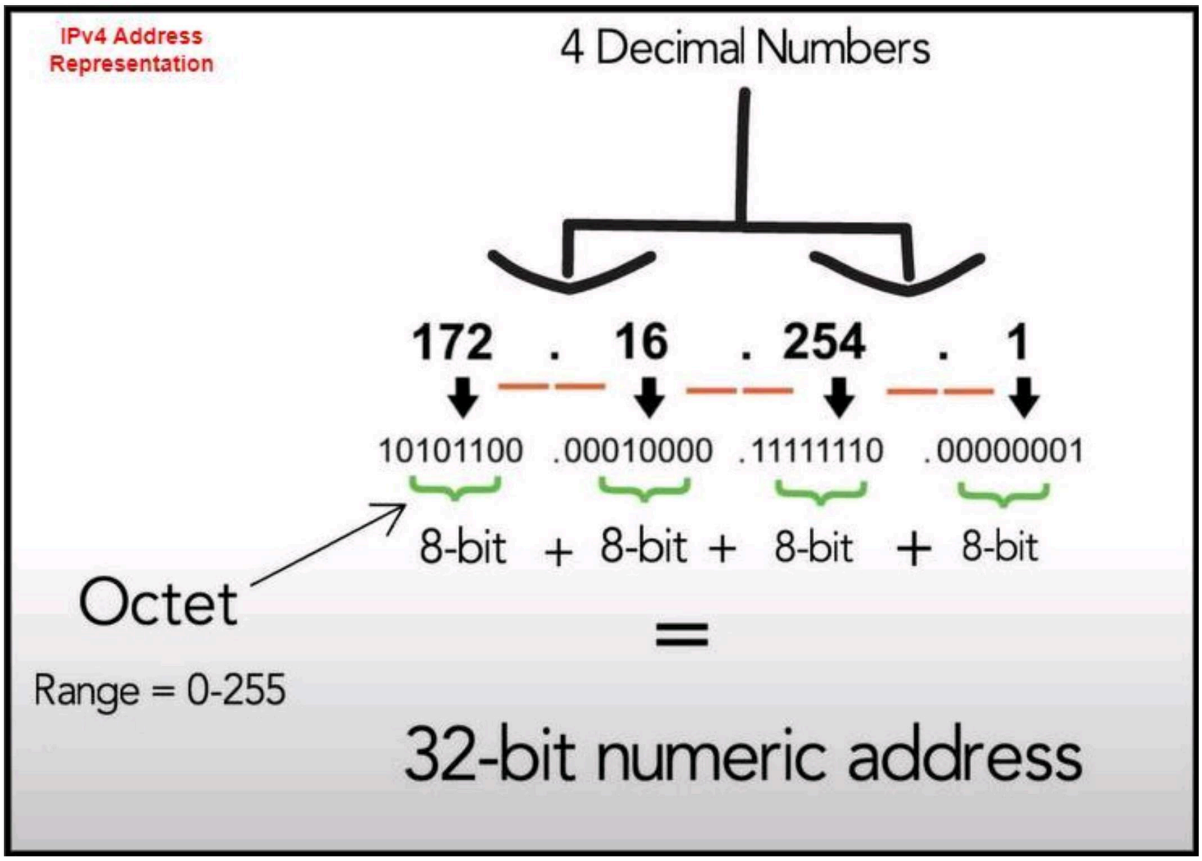
IP Address Types

Basically, there are two primary types of ip address formats used today.

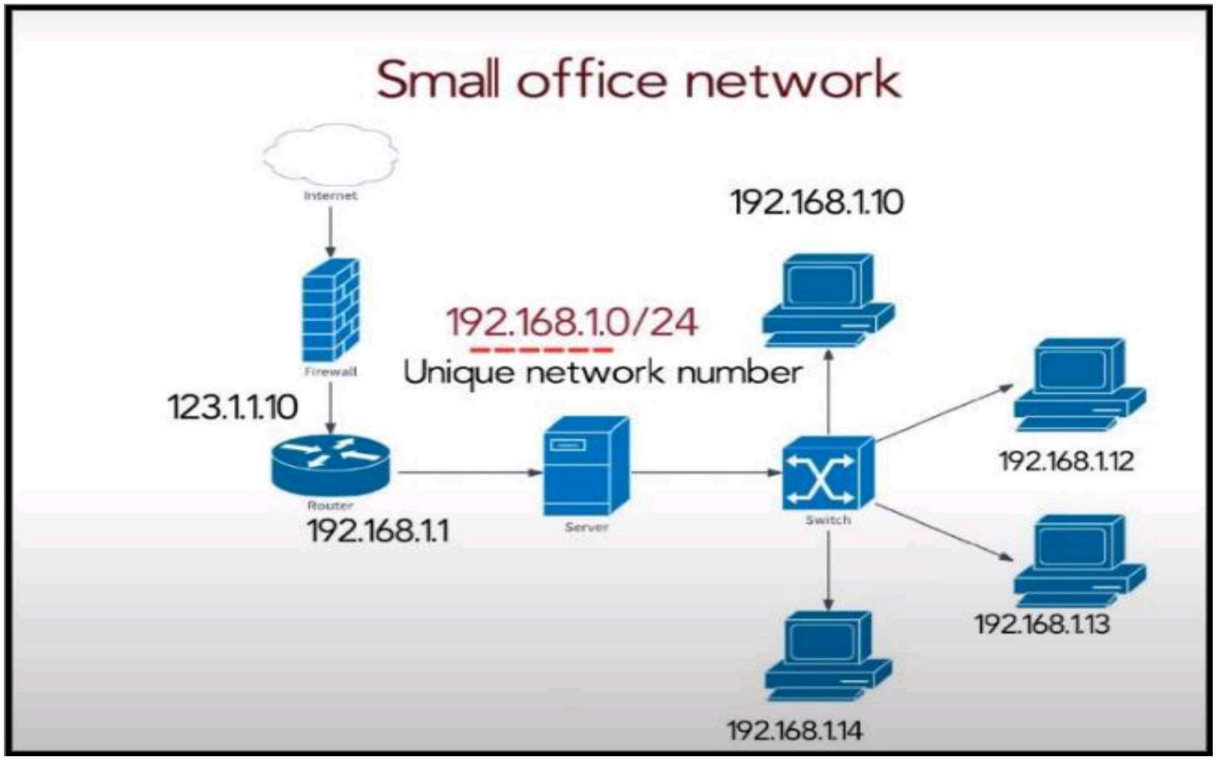
1. IPv4

2. IPv6

Refer to the following diagrams and let's understand IPv4 Address Representation



Refer to the following case-study and let's understand IPv4 Address Structure.

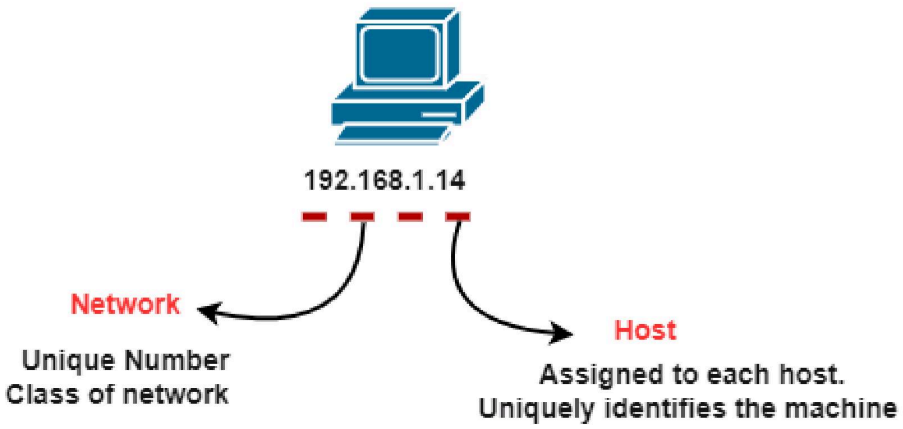


In this scenario, representing a small office network, each network running on TCP must have a unique number, and every machine on it must have a unique IP address.

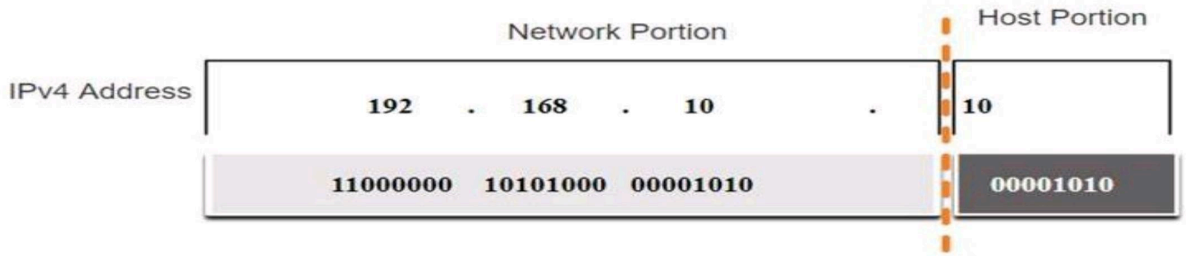
An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion.

When determining the network portion versus the host portion, you must look at the 32-bit stream.

A subnet mask is used to determine the network and host portions.

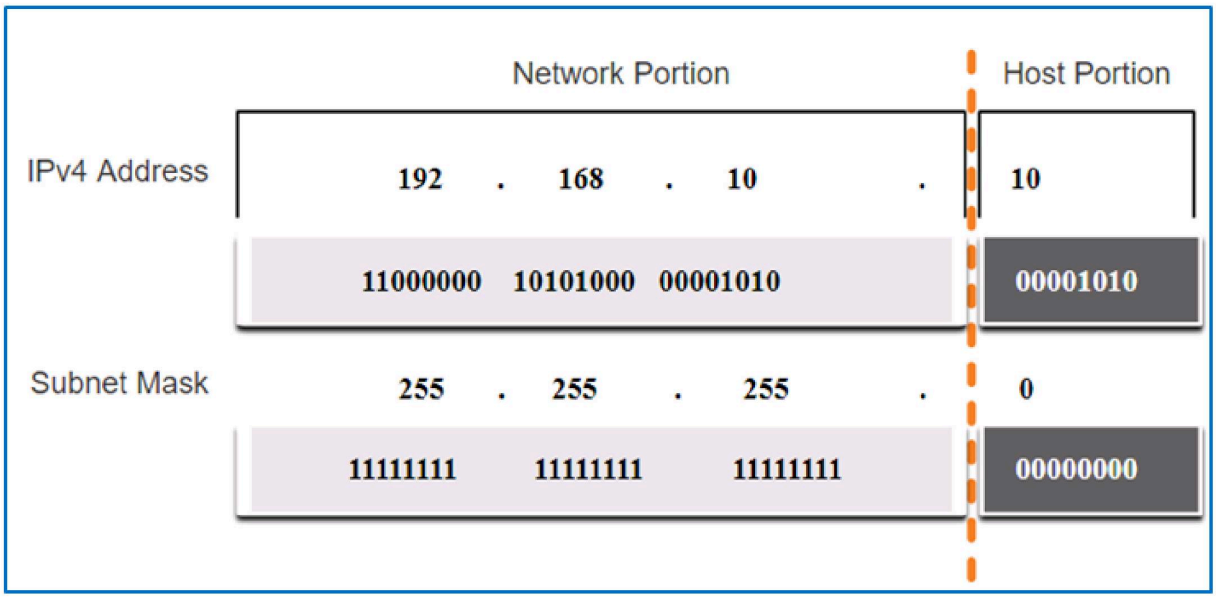


IPv4 Address Structure



IPv4 Address Structure using Binary format

IPv4 Address Structure : Subnet Mask



To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit by bit, from left to right.

The actual process used to identify the network and host portions is called ANDing.

IPv4 Address Structure: Prefix Length

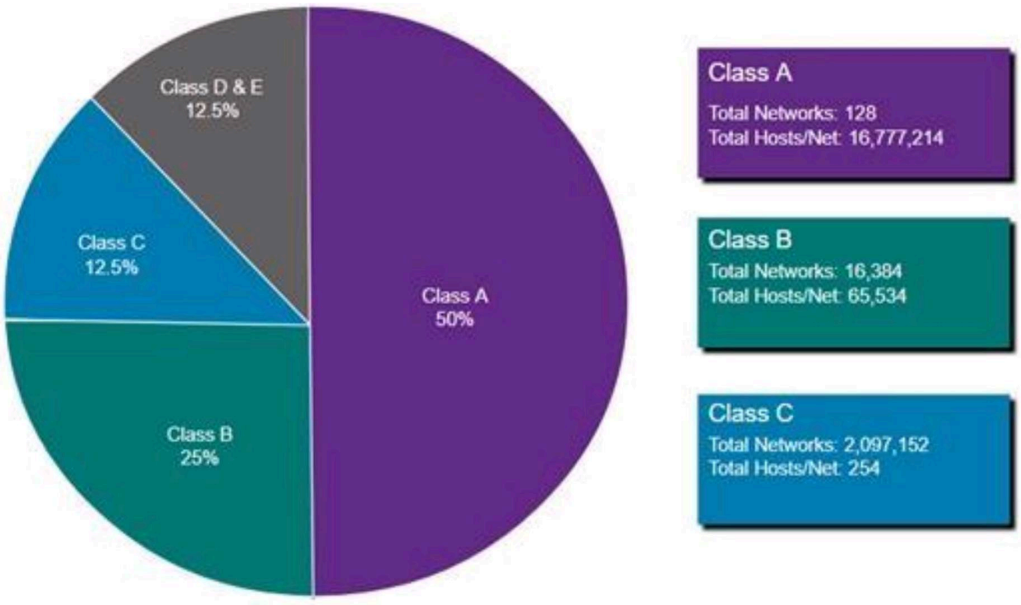
A prefix length is a less cumbersome method used to identify a subnet mask address.

The prefix length is the number of bits set to 1 in the subnet mask.

It is written in “slash notation” therefore, count the number of bits in the subnet mask and prepend it with a slash.

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29

Types of IPv4 Addresses: Legacy Classful Addressing



Classful addressing wasted many IPv4 addresses.

Classful address allocation was replaced with classless addressing which ignores the rules of classes (A, B, C).

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Exercise-1(Note: Start allocation IP address number from PC0)

Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your knowledge. Insert image below.

- Ipconfig: fill table ipconfig of all computers

PC0

Parameter	**Value**
Link local IPV6 Address	FE80::20C:CFFF:FEA2:B975
IP address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

PC1

Parameter	**Value**
Link local IPV6 Address	FE80::260:47FF:FE9D:9B9E

IP address	192.168.0.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

- Ipconfig /all: apply command on command prompt and write parameters and values in the following table.

PC0

Parameter	**Value**
Physical Address	000C.CFA2.B975
Link local IPV6 Address	FE80::20C:CFFF:FEA2:B975
IPv4 Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCPv6 Client DUID	00-01-00-01-85-63-CB-5E-00-0C-CF-A2-B9-75

PC1

Parameter	**Value**
Physical Address	0060.479D.9B9E
Link local IPV6 Address	FE80::20C:CFFF:FEA2:B975
IPv4 Address	192.168.0.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DHCPv6 Client DUID	00-01-00-01-3C-BA-CC-6E-00-60-47-9D-9B-9E

- Arp –a: before ping, write output of command from PC0 and PC1 computers

PC0

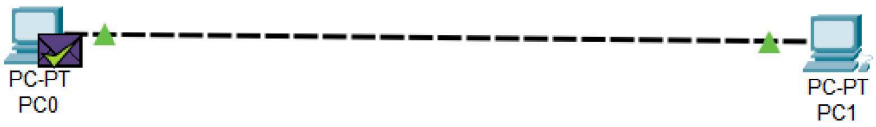
Parameter	**Value**
Internet Address	192.168.0.2
Physical Address	0060.479d.9b9e

Type	dynamic

PC1

Parameter	**Value**
Internet Address	192.168.0.1
Physical Address	000c.cfa2.b975
Type	dynamic

- Ping from PC0 to PC1 and vice versa and insert snap of output here.



- Arp –a: after ping, insert snap (below) of output of command from all computers

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.0.2           0060.479d.9b9e        dynamic
```

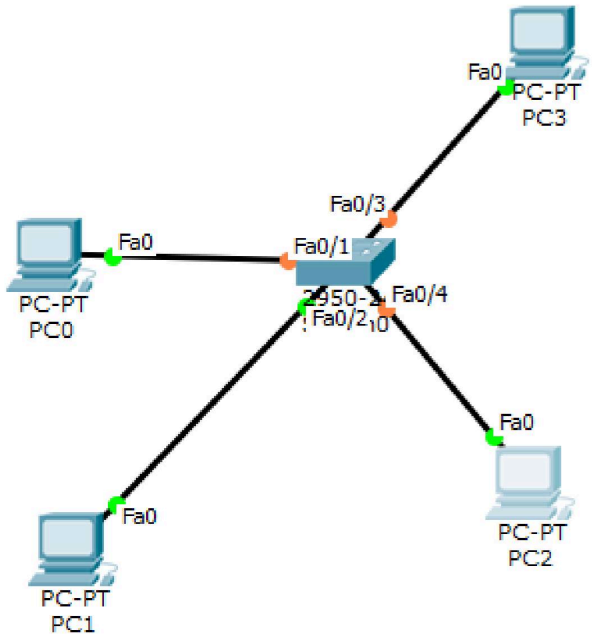
```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.0.1           000c.cfa2.b975        dynamic
```

- Netstat: insert snap of output of command from all computers\

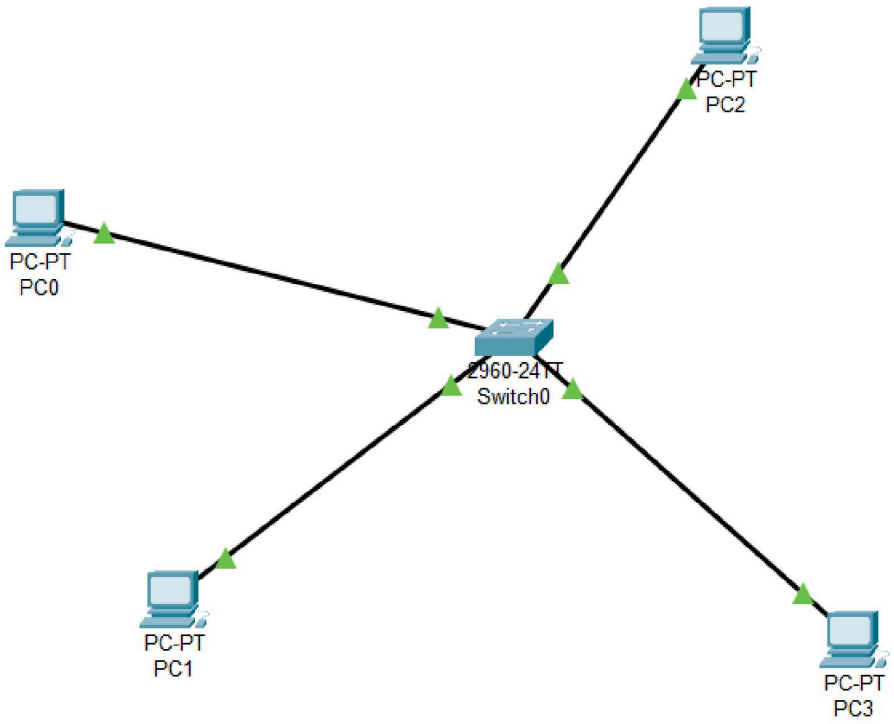
```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
```

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
```

Exercise-2: (Note: Start allocation IP address number from PC0)



Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your instruction. Insert image below.



- Ipconfig: fill table ipconfig of all computers
  PC0

Link local IPV6 Address	FE80::2E0:8FFF:FE27:7503
IP address	121.127.0.1
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0

PC1

Link local IPV6 Address	FE80::2E0:8FFF:FEAD:677E
IP address	121.127.0.2
Subnet Mask	255.0.0.0
Default Gateway	121.127.0.1

PC2

Link local IPV6 Address	FE80::201:97FF:FE1C:6785
IP address	121.127.0.3
Subnet Mask	255.0.0.0
Default Gateway	121.127.0.1

PC3

Link local IPV6 Address	FE80::290:2BFF:FE9A:536A
IP address	121.127.0.4
Subnet Mask	255.0.0.0
Default Gateway	121.127.0.1

- Ipconfig /all: apply command on command prompt and write parameters and values in following table.

PC0

Parameter	**Value**
Physical Address	00E0.8F27.7503
Link local IPV6 Address	FE80::2E0:8FFF:FE27:7503
IPv4 Address	121.127.0.1
Subnet Mask	255.0.0.0

Default Gateway	0.0.0.0
DHCPv6 Client DUID	00-01-00-01-6D-A1-14-85-00-E0-8F-27-75-03

PC1

Parameter	**Value**
Physical Address	00E0.8FAD.677E
Link local IPV6 Address	FE80::2E0:8FFF:FEAD:677E
IPv4 Address	121.127.0.2
Subnet Mask	255.0.0.0
Default Gateway	121.127.1
DHCPv6 Client DUID	00-01-00-01-04-74-AE-8B-00-E0-8F-AD-67-7E

PC2

Parameter	**Value**
Physical Address	0001.971C.6785
Link local IPV6 Address	FE80::201:97FF:FE1C:6785
IPv4 Address	121.127.0.3
Subnet Mask	255.0.0.0
Default Gateway	121.127.1
DHCPv6 Client DUID	00-01-00-01-80-3C-10-D3-00-01-97-1C-67-85

PC3

Parameter	**Value**
Physical Address	0090.2B9A.536A
Link local IPV6 Address	FE80::290:2BFF:FE9A:536A
IPv4 Address	121.127.0.4
Subnet Mask	255.0.0.0
Default Gateway	121.127.1
DHCPv6 Client DUID	00-01-00-01-CA-70-49-9B-00-90-2B-9A-53-6A

- Arp –a: before ping write/snap of output of command from all computers

```
C:\>Arp -a
No ARP Entries Found
```

- Ping from PC0 to PC1 and vice versa and get the output here.

```
Pinging 121.127.0.2 with 32 bytes of data:

Reply from 121.127.0.2: bytes=32 time<1ms TTL=128
Reply from 121.127.0.2: bytes=32 time<1ms TTL=128
Reply from 121.127.0.2: bytes=32 time<1ms TTL=128
Reply from 121.127.0.2: bytes=32 time=7ms TTL=128

Ping statistics for 121.127.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms
```

```
Pinging 127.121.0.1 with 32 bytes of data:

Reply from 127.121.0.1: bytes=32 time=3ms TTL=128
Reply from 127.121.0.1: bytes=32 time=5ms TTL=128
Reply from 127.121.0.1: bytes=32 time=3ms TTL=128
Reply from 127.121.0.1: bytes=32 time=3ms TTL=128

Ping statistics for 127.121.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

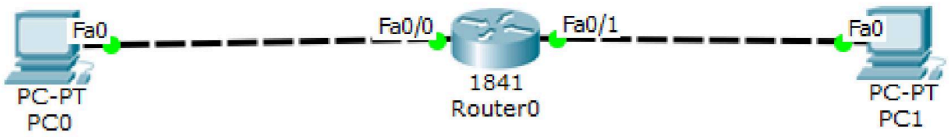
- Arp –a: after ping write/snap of output of command from all computers

```
C:\>Arp -a
  Internet Address      Physical Address      Type
  121.127.0.2           00e0.8fad.677e        dynamic
```

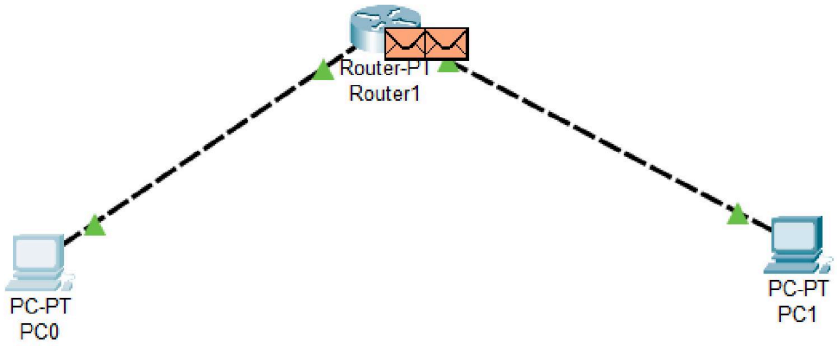
- Netstat: write/snap of output of command from all computers

```
Active Connections

  Proto  Local Address          Foreign Address        State
C:\>
```

Exercise-3 (Note: Start allocation IP address number from PC0)



Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your instruction. Insert image below.



- Ipconfig: fill following table with output of ipconfig of computer.

PC0

Link local IPV6 Address	FE80::201:64FF:FEB0:CA4B
IP address	192.168.1.20
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.100

PC1

Link local IPV6 Address	FE80::20A:41FF:FE0B:2C65
IP address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.100

- Ipconfig /all: apply command on command prompt and write parameters and values in following table

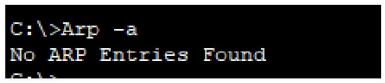
PC0

Parameter	**Value**
Physical Address	0001.64B0.CA4B
Link local IPV6 Address	FE80::201:64FF:FEB0:CA4B
IPv4 Address	192.168.1.20
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.100
DHCPv6 Client DUID	00-01-00-01-19-6B-BD-5D-00-01-64-B0-CA-4B

PC1

Parameter	**Value**
Physical Address	000A.410B.2C65
Link local IPV6 Address	FE80::20A:41FF:FE0B:2C65
IP address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.100
DHCPv6 Client DUID	00-01-00-01-B8-C9-CA-55-00-0A-41-0B-2C-65

- Arp –a: before ping write/snap of output of command from all computers



- Ping from PC0 to PC1 and vice versa and get the output here.

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time<1ms TTL=127
Reply from 192.168.1.20: bytes=32 time<1ms TTL=127
Reply from 192.168.1.20: bytes=32 time<1ms TTL=127
Reply from 192.168.1.20: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- Arp –a: after ping write/snap of output of command from all computers

```
C:\>Arp -a
  Internet Address      Physical Address      Type
  192.168.1.100         0001.6400.29e8        dynamic
```

```
C:\>Arp -a
  Internet Address      Physical Address      Type
  192.168.2.100         0010.11ca.162b        dynamic
```

- Netstat: write/snap of output of command from all computers

```
Active Connections

  Proto  Local Address          Foreign Address        State

Active Connections

  Proto  Local Address          Foreign Address        State
C:\>
```

Write answers to the following questions.

1. What are the conclusions of the ipconfig command?
   Ans: Provides basic network configuration information such as IP address, subnet mask, and default gateway.

2. What are the conclusions of **ipconfig /all** commands?
   Ans: Provides detailed network configuration information including IP address, subnet mask, default gateway, DNS server, MAC address, DHCP server, and more.

3. What are the conclusions of **arp -a** command before ping?
   Ans:Displays the current ARP cache which maps IP addresses to MAC addresses for devices the computer has recently communicated with.

4. What are the conclusions of **netstat** -r command after ping?
   Ans: Displays the routing table which shows the routes packets will take when traveling to specific IP addresses after performing a ping.

5. What is my MAC address?
   Ans: Your MAC address is a unique identifier assigned to your network interface card (NIC). You can find it using **ipconfig /all** or **ifconfig** command on Windows or Linux respectively.

6. Which network is configured? Static and Dynamic
   Ans: Static: Network configuration where IP address, subnet mask, gateway, etc., are manually set.
   Dynamic: Network configuration where IP address and other network parameters are automatically assigned by a DHCP server.

7. What is my gateway?
   Ans: Your gateway is the IP address of the device that serves as the access point to other networks, typically your router.

8. What is a hostname?
   Ans: :A hostname is a label assigned to a device connected to a computer network. It's used to identify the device within the network.

9. What is my IPv6 address?
   Ans:Your IPv6 address is a unique identifier assigned to your device on an IPv6 network. You can find it using **ipconfig /all** or **ifconfig** command.

10. What is ARPA?
    Ans:ARPA stands for Address and Routing Parameter Area. It's a top-level domain used in the reverse DNS lookup to map IP addresses to domain names.

11. What is a loopback address?
    Ans:The loopback address (127.0.0.1 for IPv4 and ::1 for IPv6) is a special address assigned to the local machine, allowing it to send data to itself.

12. What does Port 80 mean?
    Ans: Port 80 is the default port for Hypertext Transfer Protocol (HTTP), the protocol used for transmitting web pages over the internet.

13. What is the difference between logical address and physical address?

- Ans: Logical Address: Used at the network layer to uniquely identify a device on a network, e.g., IP address.
- Physical Address: Also known as MAC address, it's a hardware address assigned to the network interface card (NIC) and used at the data link layer to uniquely identify a device on a network.

14. What is NetBIOS?

    Ans: NetBIOS (Network Basic Input/Output System) is a networking protocol used for communication between devices on a local network, often used in Windows environments

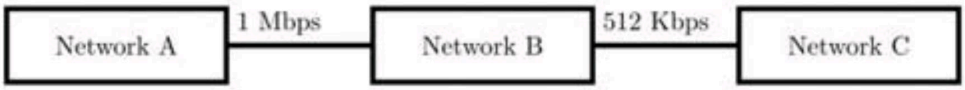
Gate Questions :

1. **Traceroute reports a possible route that is taken by packets moving from some host A to some other host B. Which of the following options represents the technique used by traceroute to identify these hosts:**

   A) By progressively querying routers about the next router on the path to B using ICMP packets, starting with the first router
   B) By requiring each router to append the address to the ICMP packet as it is forwarded to B. The list of all routers en-route to B is returned by B in an ICMP reply packet
   C) By ensuring that an ICMP reply packet is returned to A by each router en-route to B, in the ascending order of their hop distance from A
   D) By locally computing the shortest path from A to B

2. **Which of the following assertions is FALSE about the Internet Protocol (IP)?**
   A) It is possible for a computer to have multiple IP addresses
   B) IP packets from the same source to the same destination can take different routes in the network
   C) IP ensures that a packet is discarded if it is unable to reach its destination within a given number of hops
   D) The packet source cannot set the route of an outgoing packets; the route is determined only by the routing tables in the routers on the way

3. **Consider three IP networks A, B and C. Host HA in network A sends messages each containing 180 bytes of application data to a host HC in network C. The TCP layer prefixes 20 byte header to the message.**
   This passes through an intermediate network B.The maximum packet size, including 20 byte IP header, in each network is:
   A: 1000 bytes
   B: 100 bytes
   C: 1000 bytes
   The network A and B are connected through a 1 Mbps link, while B and C are connected by a 512 Kbps link (bps = bits per second).



   Assuming that the packets are correctly delivered, how many bytes, including headers, are delivered to the IP layer at the destination for one application message, in the best case? Consider only data packets.
   A) 200
   B) 220
   C) 240
   D) 260

4. **Consider three IP networks A, B and C. Host HA in network A sends messages each containing 180 bytes of application data to a host HC in network C. The TCP layer prefixes 20 byte header to the message. This passes through an intermediate network B. The maximum packet size, including 20 byte IP header, in each network, is:**
   A : 1000 bytes
   B : 100 bytes
   C : 1000 bytes
   The network A and B are connected through a 1 Mbps link, while B and C are connected by a 512 Kbps link (bps = bits per second).

   I. 

   What is the rate at which application data is transferred to host HC? Ignore errors, acknowledgments, and other overheads.
   A) 325.5 Kbps
   B) 354.5 Kbps
   C) 409.6 Kbps
   D) 512.0 Kbps

5. **In the IPv4 addressing format, the number of networks allowed under Class C addresses is:**
   A) 214
   B) 227
   C) 221
   D) 224
   Correct options. need to be changed.

6. **In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are:**
   A) Last fragment, 2400 and 2789
   B) First fragment, 2400 and 2759
   C) Last fragment, 2400 and 2759
   D) Middle fragment, 300 and 689

7. **There are n stations in slotted LAN. Each station attempts to transmit with a probability p in each time slot. What is the probability that ONLY one station transmits in a given time slot?**
   A) $np(1 - p)n-1$
   B) $(1 - p)n-1$
   C) $p(1 - p)n-1$
   D) $1 - (1 - p)n-1$

8. **The subnet mask for a particular network is 255.255.31.0. Which of the following pairs of IP addresses could belong to this network?**
   A) 172.57.88.62 and 172.56.87.23
   B) 10.35.28.2 and 10.35.29.4
   C) 191.203.31.87 and 191.234.31.88
   D) 128.8.129.43 and 128.8.161.55
9. **The routing table of a router is shown below:**

Destination	Subnet Mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
Default		Eth2

   On which interface will the router forward packets addressed to destinations 128.75.43.16 and 192.12.17.10 respectively?
   A) Eth1 and Eth2
   B) Eth0 and Eth2
   C) Eth0 and Eth3
   D) Eth1 and Eth3

10. **An organization has a class B network and wishes to form subnets for 64 departments. The subnet mask would be:**
    A) 255.255.0.0
    B) 255.255.64.0
    C) 255.255.128.0
    D) 255.255.252.0

11. **Two computers C1 and C2 are configured as follows. C1 has IP address 203.197.2.53 and netmask 255.255.128.0 .C2 has IP address 203.197.75.201 and netmask 255.255.192.0 . Which one of the following statements is true?**
    A) C1 and C2 both assume they are on the same network
    B) C2 assumes C1 is on same network, but C1 assumes C2 is on a different network
    C) C1 assumes C2 is on same network, but C2 assumes C1 is on a different network
    D) C1 and C2 both assume they are on different networks.

12. **The address of a class B host is to be split into subnets with a 6-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet?**
    A) 62 subnets and 262142 hosts.
    B) 64 subnets and 262142 hosts.
    C) 62 subnets and 1022 hosts.
    D) 64 subnets and 1024 hosts.

13. **If a class B network on the Internet has a subnet mask of 255.255.248.0 , what is the maximum number of hosts per subnet?**
    A) 1022
    B) 1023

C) 2046
D) 2047

14. Suppose computers A and B have IP addresses 10.105.1.113 and 10.105.1.91 respectively and they both use same netmask N. Which of the values of N given below should not be used if A and B should belong to the same network?

A) 255.255.255.0
B) 255.255.255.128
C) 255.255.255.192
D) 255.255.255.224

15. An Internet Service Provider (ISP) has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0/20 . The ISP wants to give half of this chunk of addresses to Organization A, and a quarter to Organization B, while retaining the remaining with itself. Which of the following is a valid allocation of addresses to A and B?

A) 245.248.136.0/21 and 245.248.128.0/22
B) 245.248.128.0/21 and 245.248.128.0/22
C) 245.248.132.0/22 and 245.248.132.0/21
D) 245.248.136.0/24 and 245.248.132.0/21

16. Consider the following routing table at an IP router:

Network No	Net Mask	Next Hop
128.96.170.0	255.255.254.0	Interface 0
128.96.168.0	255.255.254.0	Interface 1
128.96.166.0	255.255.254.0	R2
128.96.164.0	255.255.252.0	R3
0.0.0.0	Default	R4

For each IP address in Group I Identify the correct choice of the next hop from Group II using the entries from the routing table above.

Group I	Group II
i) 128.96.171.92	a) Interface 0
ii) 128.96.167.151	b) Interface 1
iii) 128.96.163.151	c) R2
iv) 128.96.164.121	d) R3
	e) R4

A) i-a, ii-c, iii-e, iv-d

B) i-a, ii-d, iii-b, iv-e

C) i-b, ii-c, iii-d, iv-e

D) i-b, ii-c, iii-e, iv-d

17. In the network 200.10.11.144/27 , the fourth octet (in decimal) of the last IP address of the network which can be assigned to a host is_____.

18. Consider three machines M, N, and P with IP addresses 100.10.5.2, 100.10.5.5 , and 100.10.5.6 respectively. The subnet mask is set to 255.255.255.252 for all the three machines. Which one of the following is true?

A) M, N, and P all belong to the same subnet
B) Only M and N belong to the same subnet
C) Only N and P belong to the same subnet
D) M, N, and P belong to three different subnets

19. An organization requires a range of IP address to assign one to each of its 1500 computers. The organization has approached an Internet Service Provider (ISP) for this task. The ISP uses CIDR and serves the requests from the available IP address space 202.61.0.0/17 . The ISP wants to assign an address space to the organization which will minimize the number of routing entries in the ISP's router using route aggregation. Which of the following address spaces are potential candidates from which the ISP can allot any one of the organization?

I. 202.61.84.0/21
II. 202.61.104.0/21
III. 202.61.64.0/21
IV. 202.61.144.0/21

A) I and II only
B) II and III only
C) III and IV only
D) I and IV only

20. A subnet has been assigned a subnet mask of 255.255.255.192 . What is the maximum number of hosts that can belong to this subnet?

A) 14
B) 30
C) 62
D) 126

21. A company has a class C network address of 204.204.204.0 . It wishes to have three subnets, one with 100 hosts and two with 50 hosts each. Which one of the following options represents a feasible set of subnet address/subnet mask pairs?

A) 204.204.204.128/255.255.255.192
204.204.204.0/255.255.255.128
204.204.204.64/255.255.255.128

B) 204.204.204.0/255.255.255.192
204.204.204.192/255.255.255.128

204.204.204.64/255.255.255.128

C) 204.204.204.128/255.255.255.128
204.204.204.192/255.255.255.192
204.204.204.224/255.255.255.192

D) 204.204.204.128/255.255.255.128
204.204.204.64/255.255.255.192
204.204.204.0/255.255.255.192

22. A subnetted Class B network has the following broadcast address: 144.16.95.255. Its subnet mask

A) is necessarily 255.255.224.0
B) is necessarily 255.255.240.0
C) is necessarily 255.255.248.0
D) could be any one of 255.255.224.0 , 255.255.240.0 ,255.255.248.0

23. Host X has IP address 192.168.1.97 and is connected through two routers R1 and R2 to another host Y with IP address 192.168.1.80. Router R1 has IP addresses 192.168.1.135 and 192.168.1.110 . R2 has IP addresses 192.168.1.67 and 192.168.1.155 . The netmask used in the network is 255.255.255.224 .

24. Given the information above, how many distinct subnets are guaranteed to already exist in the network?

A) 1
B) 2
C) 3
D) 6

25. Host X has IP address 192.168.1.97 and is connected through two routers R1 and R2 to another host Y with IP address 192.168.1.80. Router R1 has IP addresses 192.168.1.135 and 192.168.1.110 . R2 has IP addresses 192.168.1.67 and 192.168.1.155 . The netmask used in the network is 255.255.255.224 .

26. Which IP address should X configure its gateway as?

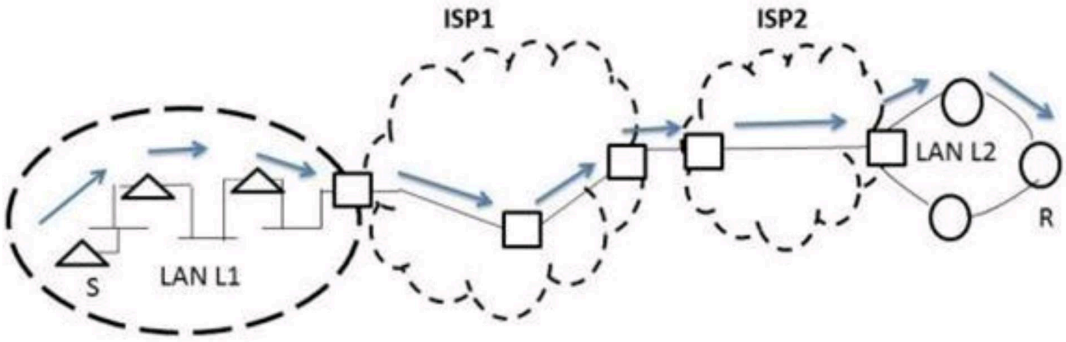
A) 192.168.1.67
B) 192.168.1.110
C) 192.168.1.135
D) 192.168.1.155

27. A computer on a 10 Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 2 Mbps. It is initially filled to capacity with 16 Megabits. What is the maximum duration for which the computer can transmit at the full 10 Mbps?

A) 1.6 seconds
B) 2 seconds
C) 5 seconds
D) 8 seconds

28. For a host machine that uses the token bucket algorithm for congestion control, the token bucket has a capacity of 1 megabyte and the maximum output rate is 20 megabytes per second. Tokens arrive at a rate to sustain output at a rate of 10 megabytes per second. The token bucket is currently full and the machine needs to send 12 megabytes of data. The minimum time required to transmit the data is _____ seconds.

29. In the diagram shown below, L1 is an Ethernet LAN and L2 is a Token-Ring LAN. An IP packet originates from sender S and traverses to R, as shown. The links within each ISP and across the two ISPs, are all point-to-point optical links. The initial value of the TTL field is 32. The maximum possible value of the TTL field when R receives the datagram is_____.



Practical-4

AIM: Understand and identify Layer-2 functionality.

Tools required:

1. Desktop Computer
2. Cisco Packet Tracer

Simulate different scenarios given below in Cisco packet tracker and fill up table.

Note: While applying IP address, student need to allocate IP address as per his/her student ID. For Example, if student ID is 20ce005 then IP address allocation for first network should start with 5.0.0.0. For subsequent network, it should start with ID+1 i.e. 6.0.0.0, 7.0.0.0. and so on.

Submission: After writing answer into this word document, Student need to change name to his ID followed by practical number. Ex 20ce005_Pr1.docx. Upload on assignment segment.
Rubrics: Nicely drafted document with clarity in answers leads to full marks. Otherwise, submission carries proportional mark.
Recommended to type, avoid copy-past to increase your typing skill.

Scenario 1: Let's assume that there are three PCs in network. All are connected with layer 2 device switch. All are assigned with the shown IP Addresses in the figure 4.1. All ARP tables are empty. Now, PC0 wants to send some data to PC2. How communication will do?

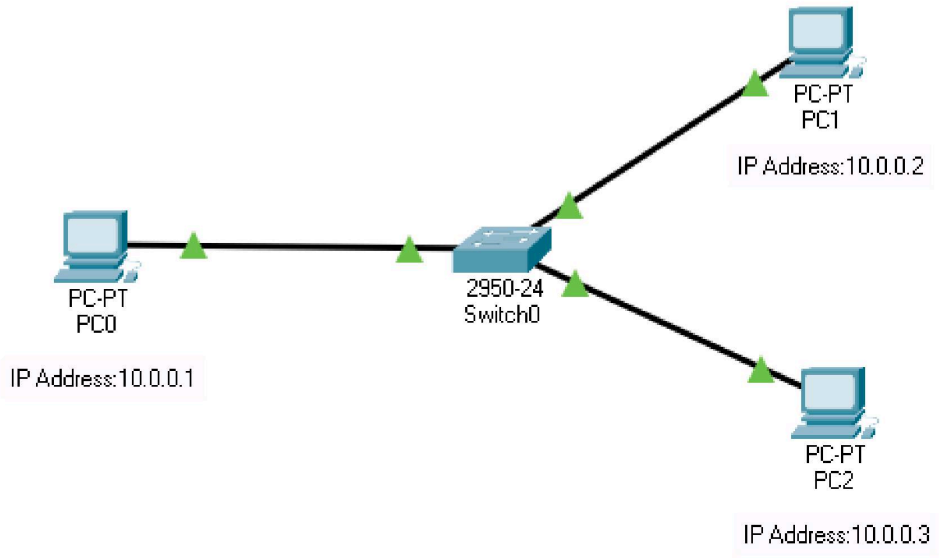


Figure 4.1 Scenario 1

Conclusion: The sender is a host and wants to send a packet to another host on the same network.

- Uses ARP to find another host's physical address

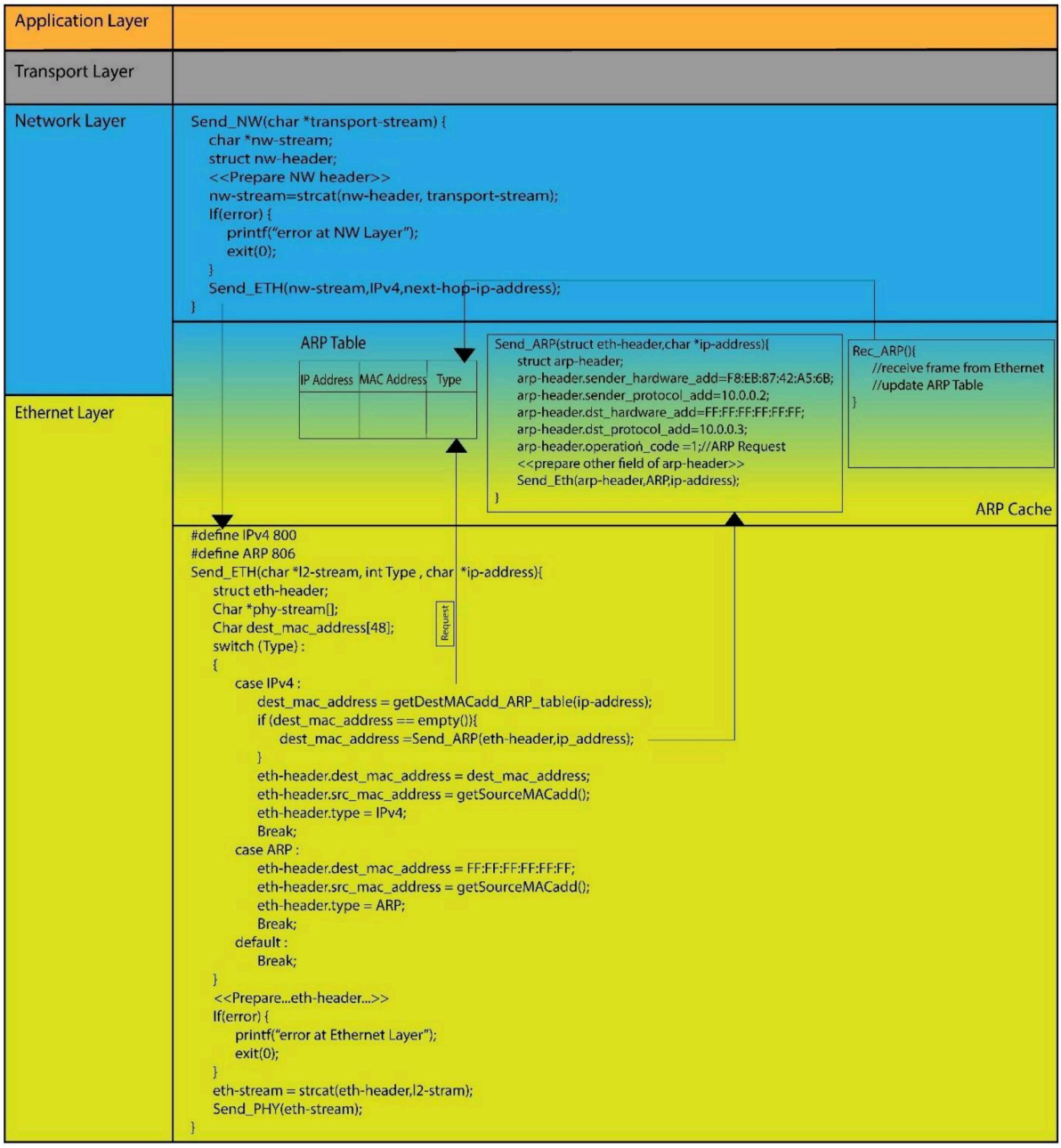


Figure 4.2 TCP/IP stack

Address Resolution Protocol (ARP):

Most of the computer programs/applications use logical address (IP address) to send/receive messages, however, the actual communication happens over the physical address (MAC address) i.e., from layer 2 of the TCP/IP model. So, our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical addresses.

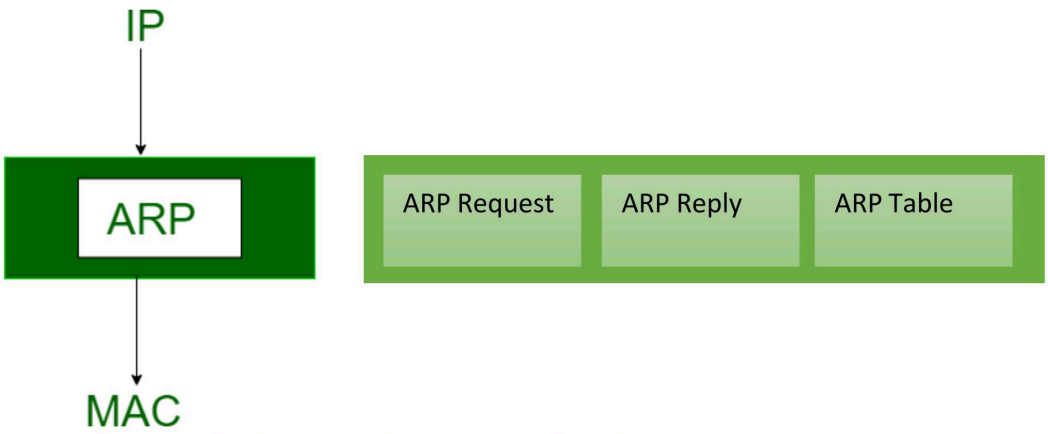


Figure 4.3 ARP Maps IP address to MAC address

The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Network layer in the OSI model.
ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.

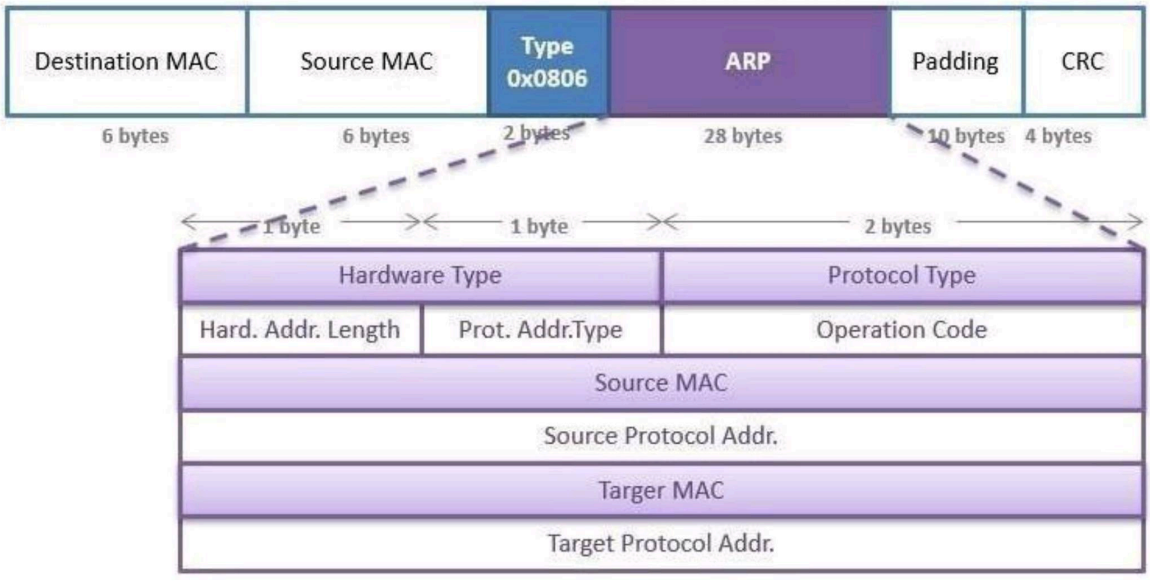


Figure 4.4 ARP header

Scenario 2: With respect to given topology shown in figure 4.5, IP addresses are assigned to all the PCs. Initial ARP tables are empty. Now, PC0 wants to send data to PC3. Write down the step how communication will take place.

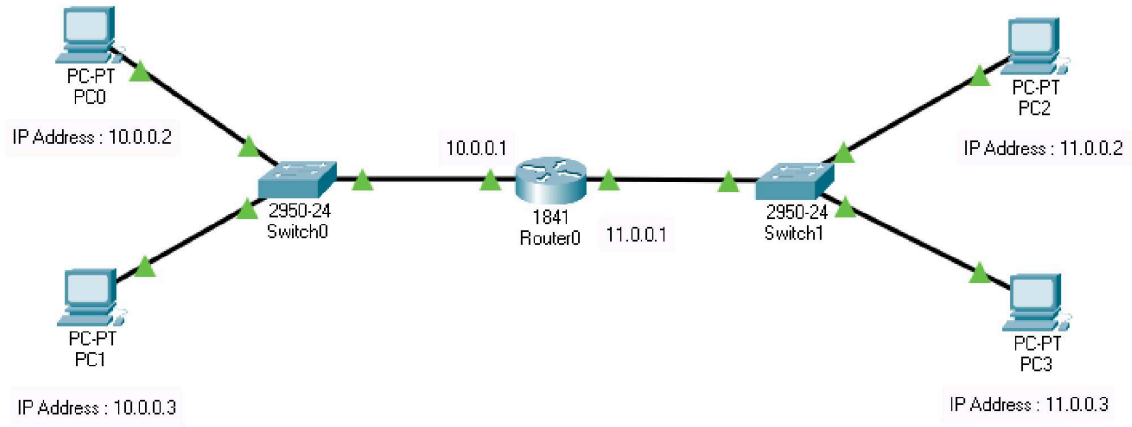


Figure 4.5 Scenario 2

Conclusion: The sender is a host and wants to send a packet to another host on another network.

- The sender looks at its routing table.
- Find the IP address of the next-hop (router) for this destination.
- Use ARP to find the router's physical address

Scenario 3: With respect to given topology shown in figure 4.6, IP addresses are assigned to all the PCs. Initial ARP tables are empty. Now, Packet is received by router 1 with destination IP address 12.0.0.2. Write down the step how communication will take place.

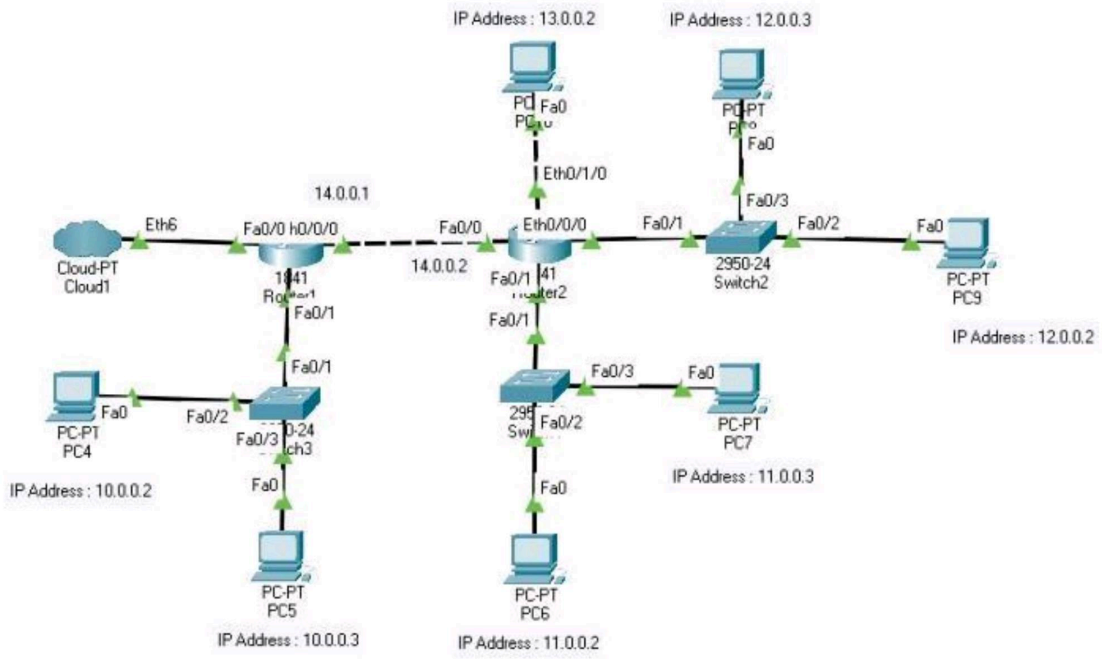


Figure 4.6 Scenario 3

Conclusion: the sender is a router and received a datagram destined for a host on another network.

- The router checks its routing table.
- Find the IP address of the next router.
- Use ARP to find the next router's physical address.

Question 1: List out Different network devices and give a small introduction of the same.

Ans. Router: Routes data between different networks at the network layer (Layer 3).

1. **Switch**: Connects devices within a local area network (LAN) at the data link layer (Layer 2), forwarding data based on MAC addresses.
2. **Hub**: Simple device that connects multiple devices in a LAN but broadcasts data to all connected devices, operating at the physical layer (Layer 1).
3. **Modem**: Converts digital data from a computer into analog signals for transmission over communication lines, and vice versa, enabling internet connectivity.
4. **Access Point (AP)**: Provides Wi-Fi connectivity, allowing wireless devices to connect to a wired network.

Question 2: write down difference between HUB and SWITCH.

Ans. Here are the key differences between a hub and a switch:

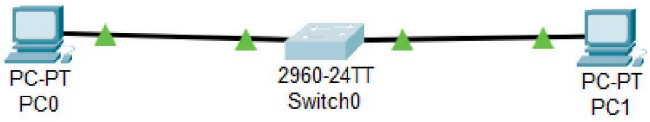
1. **Functionality**:
    - Hub: Operates at the physical layer (Layer 1) of the OSI model and simply forwards data to all connected devices without any intelligence. It broadcasts data to all ports.
    - Switch: Operates at the data link layer (Layer 2) of the OSI model and intelligently forwards data to the specific device it is intended for based on the device's MAC address. It creates a dedicated connection between the sender and receiver, reducing unnecessary traffic.
2. **Broadcasting**:
    - Hub: Broadcasts data to all connected devices, causing network congestion and reducing overall network efficiency.
    - Switch: Forwards data only to the specific device it is intended for, eliminating unnecessary broadcasting and improving network performance.
3. **Bandwidth Management**:
    - Hub: Shares available bandwidth among all connected devices, leading to potential bandwidth bottlenecks and slower network speeds.
    - Switch: Provides dedicated bandwidth to each port, allowing devices to communicate simultaneously without sharing bandwidth. This results in faster and more efficient data transfer.
4. **Collision Domain**:

- Hub: All devices connected to a hub belong to a single collision domain, meaning that data collisions can occur when multiple devices attempt to transmit data simultaneously.
- Switch: Each port on a switch is in its own collision domain, significantly reducing the likelihood of data collisions and improving network reliability.

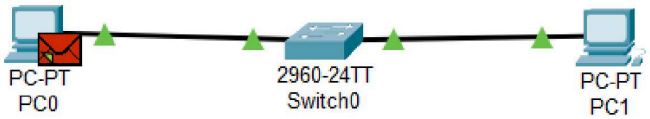
5. **Security**:
    - Hub: Lacks security features and does not provide any means of controlling or securing data transmission.
    - Switch: Offers better security by isolating traffic between devices and preventing unauthorized access to data transmitted between them.

Exercise-1

Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your knowledge.



Ping from PC0 to PC1 and vice versa and insert snap of output here.



Write down ARP table of PC0 and PC1.

Fill ARP table entry of PC0

IP address	MAC Address
121.127.1.1	0003.e49b.c8ca

Fill ARP table entry of PC1

IP address	MAC Address
121.127.1.2	00e0.8fb6.b613

Questions:

1. What does ARP table contain?
   Ans :The ARP (Address Resolution Protocol) table contains mappings between IP addresses and corresponding MAC (Media Access Control) addresses on a local network. It essentially acts as a cache that helps devices on a network quickly determine the MAC address associated with a particular IP address.

2. Why there is need of ARP table?
   Ans :The ARP table is needed because it allows devices on a network to efficiently communicate with each other. When a device wants to send data to another device on the same network, it needs to know the MAC address of the recipient. The ARP table helps in quickly resolving IP addresses to MAC addresses, reducing the need for constant broadcasting of ARP requests.

3. What is topology name of exercise-1?
   Ans: Star Topology

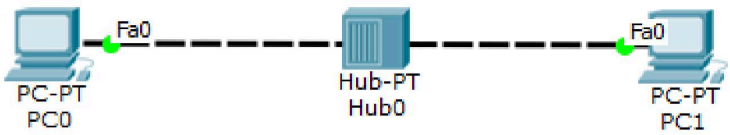
4. What is relation of IP address with MAC address?
   Ans :The IP address (Internet Protocol address) and MAC address (Media Access Control address) are both used in network communication, but they serve different purposes. An IP address is a logical address assigned to a device for communication within an IP network, while a MAC address is a unique identifier assigned to network interfaces for communication on the physical network. The relation between them is that ARP (Address Resolution Protocol) is used to map IP addresses to MAC addresses on a local network.

5. Can we change MAC Address of machine?
   Ans: Yes, it is possible to change the MAC address of a machine. This process is known as MAC address spoofing. However, it's worth noting that MAC addresses are typically hardcoded into network interface hardware and changing them may violate network policies or cause network connectivity issues.

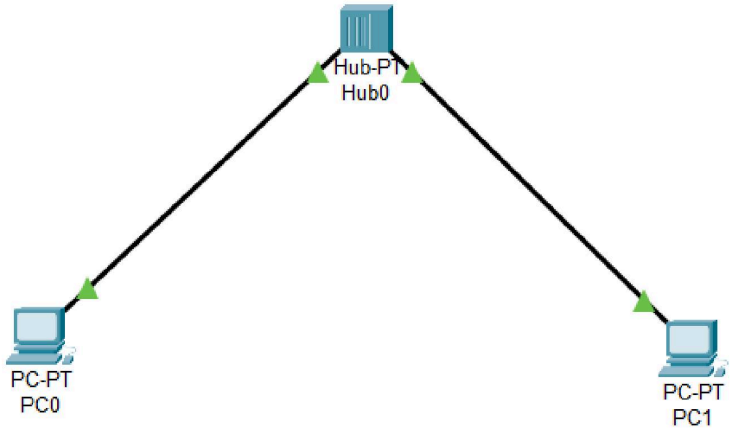
6. Can we change IP address of machine?

   Ans: Yes, it is possible to change the IP address of a machine. IP addresses can be assigned statically or dynamically, and in either case, they can be changed by network administrators or users with appropriate permissions. However, changing the IP address may require reconfiguring network settings and could potentially disrupt network connectivity until the new address is properly propagated and recognized by other devices on the network.

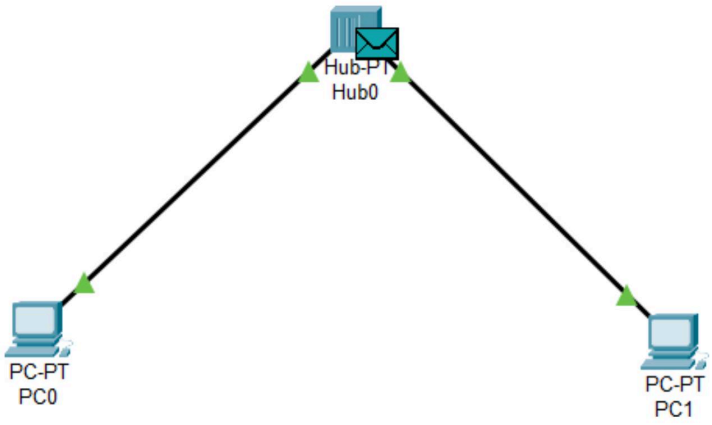
Exercise-2 :



Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your knowledge.



Ping from PC0 to PC1 and vice versa and insert snap of output here.



Write down ARP table of PC0 and PC1. Write down switch table of Hub0.
Fill ARP table entry of PC0

IP address	MAC Address
121.127.1.1	0007.ecb4.12b8

Fill ARP table entry of PC1

IP address	MAC Address
121.127.1.2	0010.114b.c508

Questions:

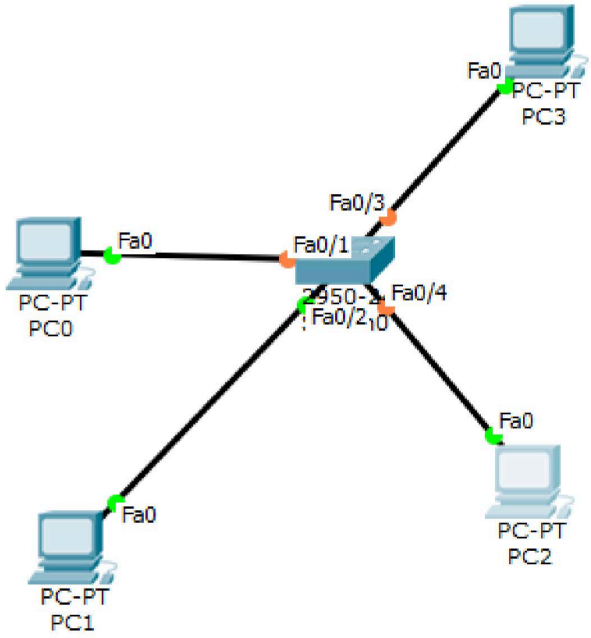
1. What is functionality of Hub?
   Ans :A hub operates at the physical layer (Layer 1) of the OSI model and functions as a central connection point for multiple devices in a network. Its primary functionality is to receive data from one device connected to its port and broadcast it to all other devices connected to its other ports. Essentially, it blindly forwards data packets without any intelligence or processing, leading to inefficient use of network bandwidth.

2. Does hub have IP address?
   Ans: No, a hub does not have its own IP address. Hubs operate at the physical layer of the OSI model and do not have the capability to understand or process IP addresses. They simply pass along data frames based on the MAC addresses of connected devices without any knowledge of IP addresses.

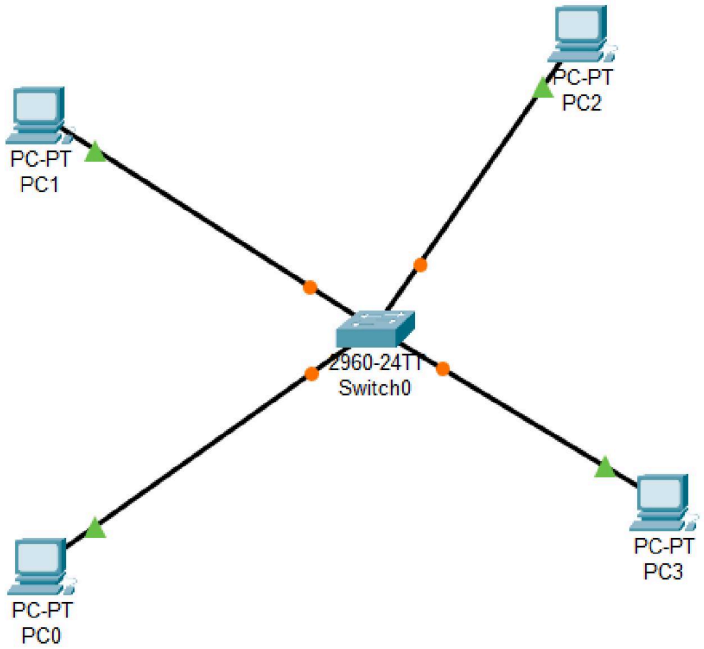
3. Does hub have switch (ARP) table?
   Ans: No, hubs do not have a switch table or an ARP (Address Resolution Protocol) table. Unlike switches, which operate at the data link layer (Layer 2) and maintain tables for mapping MAC addresses to port locations, hubs do not perform any intelligent forwarding or address resolution. They simply broadcast incoming data packets to all connected devices.

4. What is topology of exercise-2?
   Ans: Star Topology

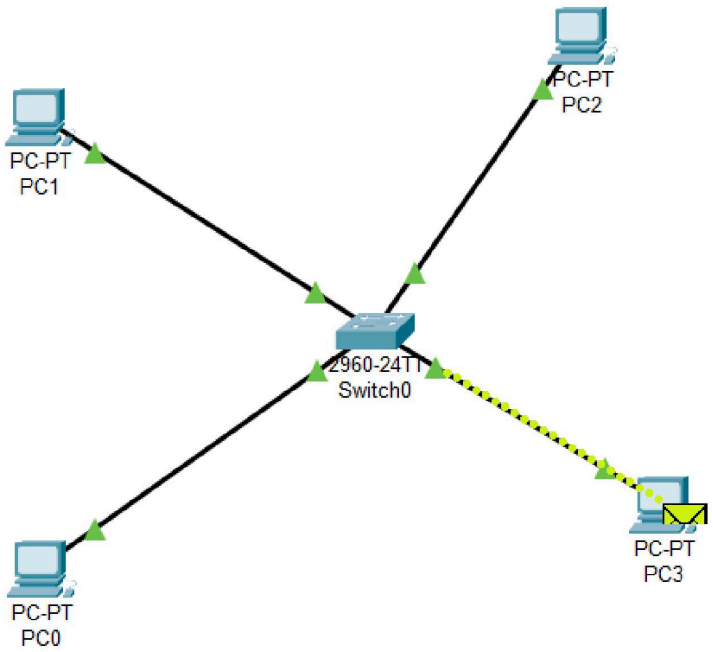
Exercise-3

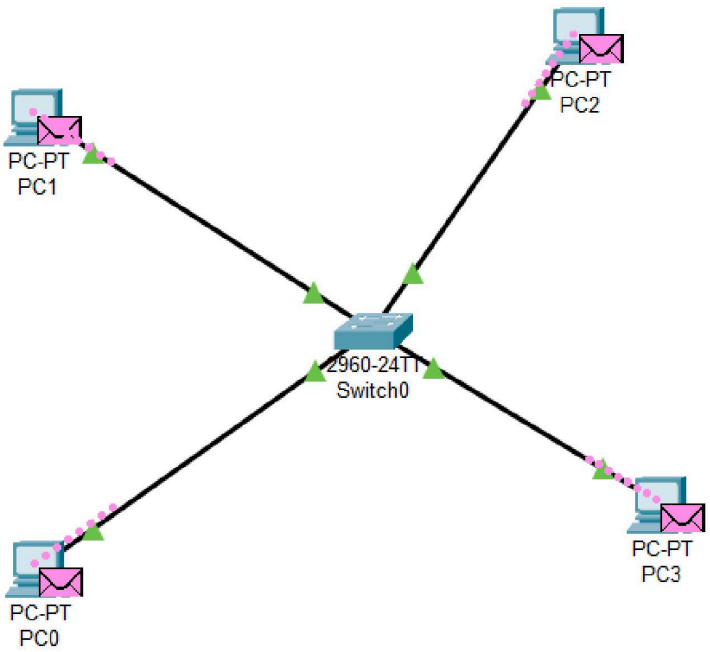


Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your knowledge.



Ping from PC0,PC1,PC2 and PC3 respectively and insert snap of output here.





11

Write down ARP tables of PC0,PC1,PC2 and PC3. Write down switch table of Switch0.
Fill ARP table entry of PC0

IP address	MAC Address
121.127.1.1	000b.be79.8c3a

Fill ARP table entry of PC1

IP address	MAC Address

121.127.1.3	0030.f26e.b2e9

Fill ARP table entry of PC2

IP address	MAC Address
121.127.1.2	00e0.f70c.b947

Fill ARP table entry of PC3

IP address	MAC Address
11.127.1.1	0050.0fe1.9b6a

Fill Switch table entry of Switch0

MAC Address	Ethernet port no
00:09:7c:75:6B:25	26

Questions:

1. What is functionality of switch?
   Ans: A switch operates at the data link layer (Layer 2) of the OSI model and functions as a central connection point for devices within a local area network (LAN). Its primary functionality is to receive data frames from connected devices and intelligently forward them to their intended destination based on the destination MAC address. Switches maintain a MAC address table, also known as a switch table, to facilitate efficient data forwarding, leading to better network performance and reduced collisions compared to hubs.

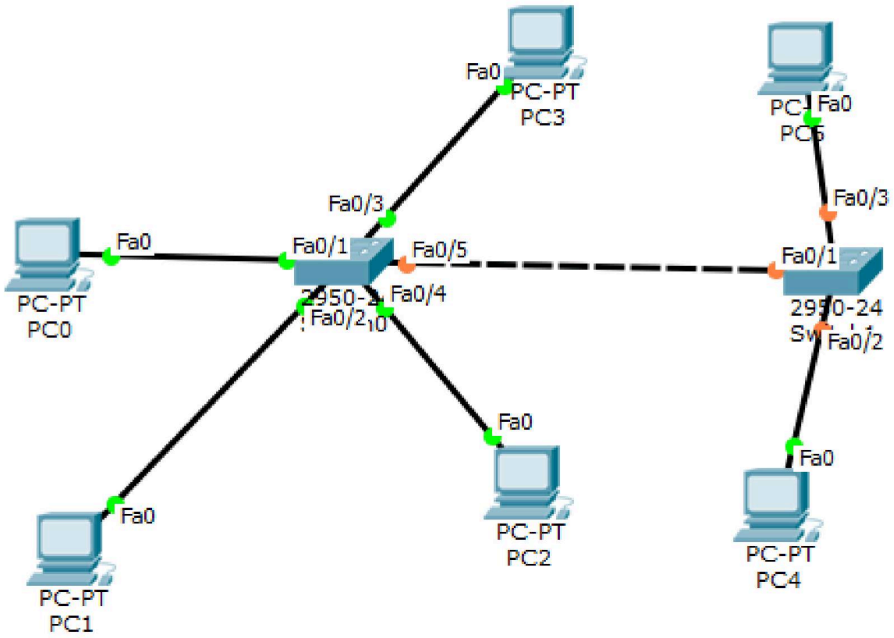
2. Does switch have IP address?
   Ans: Yes, switches can have IP addresses, particularly if they are managed switches. Managed switches often include features such as remote management, VLAN configuration, and network monitoring, which require an IP address for configuration and access purposes. Unmanaged switches typically do not have their own IP addresses and operate in a plug-and-play fashion.

3. Does switch have switch (ARP) table?
   Ans:Yes , switches maintain a switch table, sometimes referred to as a MAC address table or ARP table. This table maps MAC addresses to the physical ports on the switch. When a switch receives a data frame, it checks the destination MAC address against its switch table to determine the outgoing port. If the MAC address is not found in the table, the switch may use ARP (Address Resolution Protocol) to discover the MAC address associated with the destination IP address.

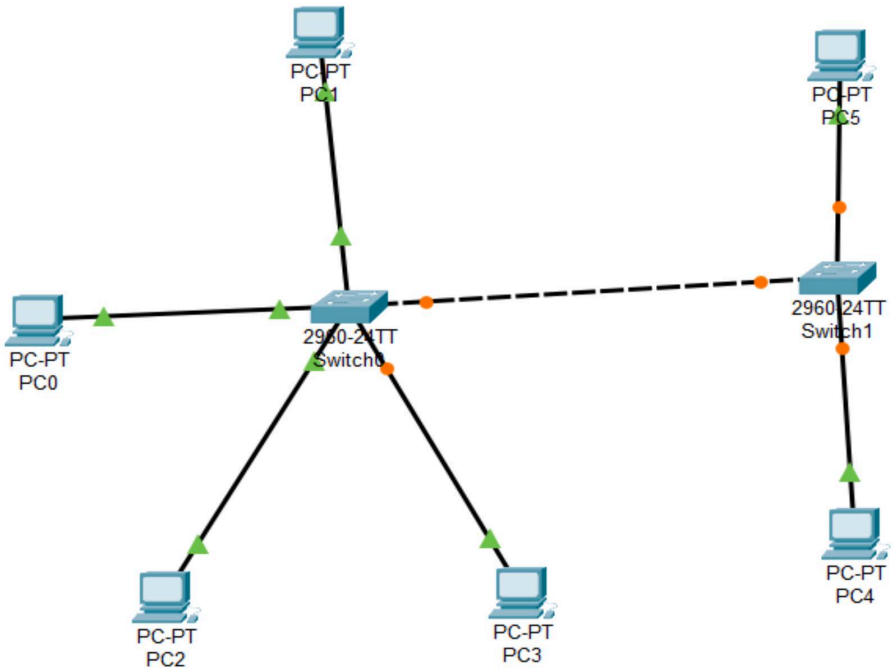
4. What is topology name of exercise-3?

   Ans: Star Topology

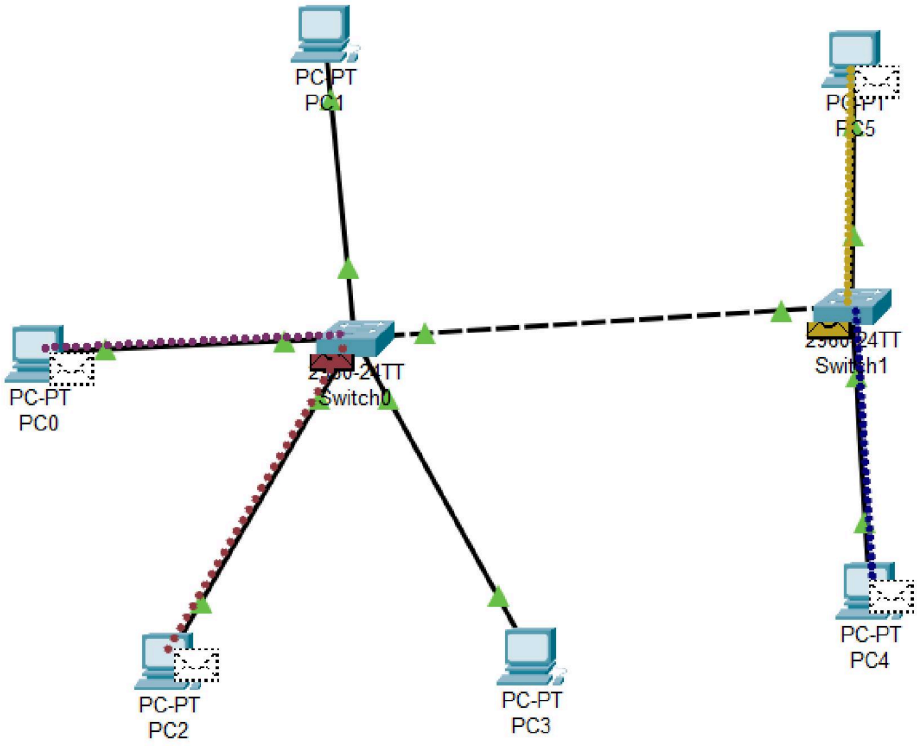
Exercise-4



Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your knowledge.



Ping from all given PCs respectively and insert snap of output here.



Write down ARP table of all given PCs. Write down switch table of Switch0 and Switch1.
ARP table entry of PC0

IP address	MAC Address
10.10.1.4	0050.0f78.b73d
10.11.1.2	0001.96b9.c3ea

ARP table entry of PC1

IP address	MAC Address
10.10.1.3	0002.1747.d70c

ARP table entry of PC2

IP address	MAC Address
10.10.1.2	0005.5e74.200d

ARP table entry of PC3

IP address	MAC Address
10.10.1.1	0002.17bb.2975

ARP table entry of PC4

IP address	MAC Address
10.10.1.1	0002.17bb.2975

ARP table entry of PC5

IP address	MAC Address
10.11.1.2	0001.96b9.c3ea

Switch table entry of Switch0

MAC Address	Ethernet port no
00:90:0c:13:69:ID	26

Switch table entry of Switch1

MAC Address	Ethernet port no
00:D0:D3:A4:37:BD	26

Questions

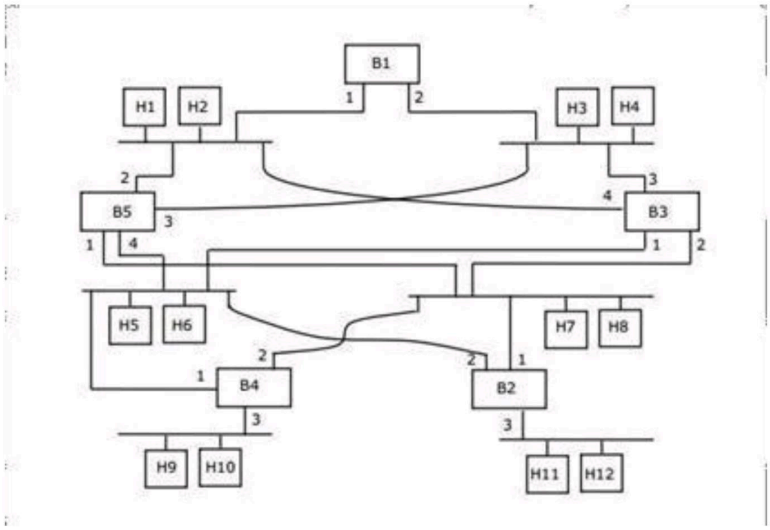
1. Does both the switch will have identical switching table?
   Ans: No, the switching tables on two different switches may not be identical. Switching tables are dynamically built based on the MAC addresses observed on each switch's ports. They reflect the devices connected to each switch and their corresponding MAC addresses. While switches in the same network may have some overlap in their switching tables, they can differ due to variations in connected devices, network traffic patterns, and the timing of MAC address learning.

2. In Exercise-4, why does PC0 contain IP MAC address of PC4?
   Ans : As it sends packets from pc0 to pc4.

3. What is topology name of exercise-4?
   Ans: Hybrid Topology

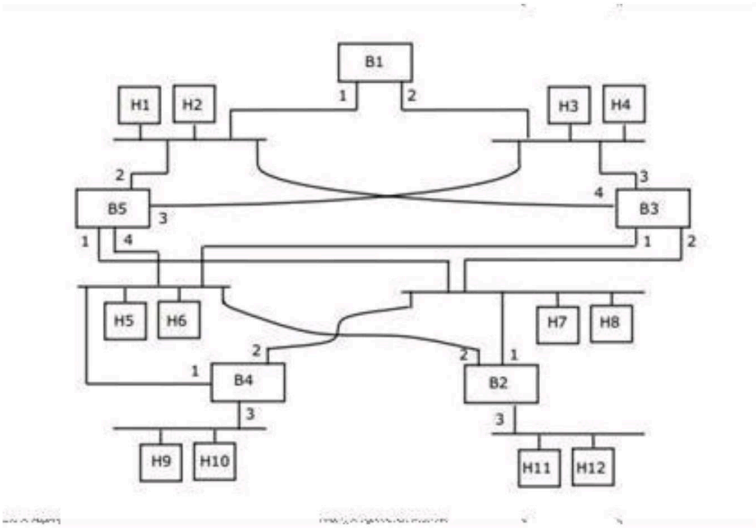
GATE Questions:

1. **Consider the diagram shown below where a number of LANs are connected by (transparent) bridges. In order to avoid packets looping through circuits in the graph, the bridges organize themselves in a spanning tree. First, the root bridge is identified as the bridge with the least serial number. Next, the root sends out (one or more) data units to enable the setting up of the spanning tree of shortest paths from the root bridge to each bridge.**
   Each bridge identifies a port (the root port) through which it will forward frames to the root bridge. Port conflicts are always resolved in favour of the port with the lower index value. When there is a possibility of multiple bridges forwarding to the same LAN (but not through the root port), ties are broken as follows: bridges closest to the root get preference and between such bridges, the one with the lowest serial number is preferred.



   For the given connection of LANs by bridges, which one of the following choices represents the depth first traversal of the spanning tree of bridges?
   A) B1, B5, B3, B4, B2
   B) B1, B3, B5, B2, B4
   C) B1, B5, B2, B3, B4
   D) B1, B3, B4, B5, B2
   Ans.

2. **Consider the diagram shown below where a number of LANs are connected by (transparent) bridges. In order to avoid packets looping through circuits in the graph, the bridges organize themselves in a spanning tree. First, the root bridge is identified as the bridge with the least serial number. Next, the root sends out (one or more) data units to enable the setting up of the spanning tree of shortest paths from the root bridge to each bridge. Each bridge identifies a port (the root port) through which it will forward frames to the root bridge. Port conflicts are always resolved in favour of the port with the lower index value. When there is apossibility of multiple bridges forwarding to the same LAN (but not through the root port), ties are broken as follows: bridges closest to the root get preference andbetween such bridges, the one with the lowest serial number is preferred.**



Consider the spanning tree B1, B5, B3, B4, B2 for the given connection of LANs by bridges that represents the depth first traversal of the spanning tree of bridges. Let host H1 send out a broadcast ping packet. Which of the following options represents the correct forwarding table on B3?

A)

Hosts	Port
H1, H2, H3, H4	3
H5, H6, H9, H10	1
H7, H8, H11, H12	2

B)

Hosts	Port
H1, H2	4
H3, H4	3
H5, H6	1
H7, H8, H9, H10, H11, H12	2

C)

Hosts	Port
H3, H4	3
H5, H6, H9, H10	1
H1, H2	4
H7, H8, H11, H12	2

D)

Hosts	Port
H1, H2, H3, H4	3
H5, H7, H9, H10	1
H7, H8, H11, H12	4

A) A
B) B
C) C
D) D
Ans.

3. **Consider a simple communication system where multiple nodes are connected by a shared broadcast medium (like Ethernet or wireless). The nodes in the system use the following carrier-sense based medium access protocol. A node that receives a packet to transmit will carrier-sense the medium for 5 units of time. If the node does not detect any other transmission, it starts transmitting its packet in the next time unit. If the node detects another transmission, it waits until this other transmission finishes, and then begins to carrier-sense for 5 time units again. Once they start to transmit, nodes do not perform any collision detection and continue transmission even if a collision occurs. All transmissions last for 20 units of time. Assume that the transmission signal travels at the speed of 10 meters per unit time in the medium.**

   Assume that the system has two nodes P and Q, located at a distance d meters from each other. P start transmitting a packet at time t = 0 after successfully completing its carrier-sense phase. Node Q has a packet to transmit at time t = 0 and begins to carrier- sense the medium.

   The maximum distance d (in meters, rounded to the closest integer) that allows Q to successfully avoid a collision between its proposed transmission and P 'songoing transmission is_____.

   Ans.

4. **A and B are the only two stations on an Ethernet. Each has a steady queue of frames to send. Both A and B attempt to transmit a frame, collide, and A wins the first backoff race. At the end of this successful transmission by A, both A and B attempt to transmit and collide. The probability that A wins the second backoff race is:**
   A) 0.5
   B) 0.625
   C) 0.75
   D) 1.0
   Ans.

5. **Which of the following statements is TRUE?**
   A) Both Ethernet frame and IP packet include checksum fields
   B) Ethernet frame includes a checksum field and IP packet includes a CRC field
   C) Ethernet frame includes a CRC field and IP packet includes a checksum field
   D) Both Ethernet frame and IP packet include CRC fields
   Ans.

6. **Consider three IP networks A, B and C. Host HA in network A sends messages each containing 180 bytes of application data to a host HC in network C. The TCP layer prefixes 20 byte header to the message.**
   This passes through an intermediate network B.The maximum packet size, including 20 byte IP header, in each network is:
   A: 1000 bytes
   B: 100 bytes
   C: 1000 bytes

The network A and B are connected through a 1 Mbps link, while B and C are connected by a 512 Kbps link (bps = bits per second).

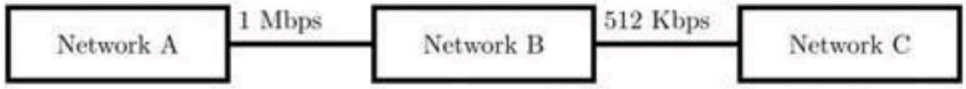
Assuming that the packets are correctly delivered, how many bytes, including headers, are delivered to the IP layer at the destination for one application message, in the best case? Consider only data packets.

A) 200
B) 220
C) 240
D) 260
Ans.

7. **Consider three IP networks A, B and C. Host HA in network A sends messages each containing 180 bytes of application data to a host HC in network C. The TCP layer prefixes 20 byte header to the message. This passes through an intermediate network B. The maximum packet size, including 20 byte IP header, in each network, is:**

   A : 1000 bytes
   B : 100 bytes
   C : 1000 bytes

   The network A and B are connected through a 1 Mbps link, while B and C are connected by a 512 Kbps link (bps = bits per second).



   What is the rate at which application data is transferred to host HC? Ignore errors, acknowledgments, and other overheads.

   A) 325.5 Kbps
   B) 354.5 Kbps
   C) 409.6 Kbps
   D) 512.0 Kbps
   Ans.

8. **A 2 km long broadcast LAN has 107 bps bandwidth and uses CSMA/CD. The signal travels along the wire at 2 × 108 m/s. What is the minimum packet size that can be used on this network?**

   A) 50 bytes
   B) 100 bytes
   C) 200 bytes
   D) None of the above
   Ans.

9. **Consider that 15 machines need to be connected in a LAN using 8-port Ethernet switches. Assume that these switches do not have any separate uplink ports. The minimum number of switches needed is_____.**
   Ans.

10. **A host is connected to a Department network which is part of a University network. The University network, in turn, is part of the Internet. The largest network in which the Ethernet address of the host is unique is:**
    A) the subnet to which the host belongs
    B) the Department network
    C) the University network
    D) the Internet
    Ans.

11. **Which of the following statements is FALSE regarding a bridge?**
    A) Bridge is a layer 2 device
    B) Bridge reduces collision domain
    C) Bridge is used to connect two or more LAN segments
    D) Bridge reduces broadcast domain
    Ans.

12. **Suppose the round trip propagation delay for a 10 Mbps Ethernet having 48-bit jamming signal is 46.4 μs. The minimum frame size is:**
    A) 94
    B) 416
    C) 464
    D) 512
    Ans.

13. **A link has transmission speed of 106 bits/sec. It uses data packets of size 1000 bytes each. Assume that the acknowledgment has negligible transmission delay and that its propagation delay is the same as the data propagation delay. Also, assume that the processing delays at nodes are negligible. The efficiency of the stop-and-wait protocol in this setup is exactly 25%. The value of the one way propagation delay (in milliseconds) is_____.**
    Ans.

14. **Consider a simplified time slotted MAC protocol, where each host always has data to send and transmits with probability p = 0.2 in every slot. There is no backoff and one frame can be transmitted in one slot. If more than one host transmits in the same slot, then the transmissions are unsuccessful due to collision. What is the maximum number of hosts which this protocol can support if each host has to be provided a minimum throughput of 0.16 frames per time slot?**
    A) 1
    B) 2
    C) 3
    D) 4
    Ans.

15. In a TDM medium access control bus LAN, each station is assigned one time slot per cycle for transmission. Assume that the length of each time slot is the time to transmit 100 bitsplus the end-to-end propagation delay. Assume a propagation speed of 2 × 108m/sec. The length of the LAN is 1 km with a bandwidth of 10 Mbps. The maximum number of stations that can be allowed in the LAN so that the throughput of each station can be 2/3 Mbpsis

A) 3
B) 5
C) 10
D) 20
Ans.

16. The address resolution protocol (ARP) is used for:

A) Finding the IP address from the DNS
B) Finding the IP address of the default gateway
C) Finding the IP address that corresponds to a MAC address
D) Finding the MAC address that corresponds to an IP address
Ans.

17. Suppose that in an IP-over-Ethernet network, a machine X wishes to find the MAC address of another machine Y in its subnet. Which one of the following techniques can be used for this?

A) X sends an ARP request packet to the local gateway's IP address which then finds the MAC address of Y and sends to X
B) X sends an ARP request packet to the local gateway's MAC address which then finds the MAC address of Y and sends to X
C) X sends an ARP request packet with broadcast MAC address in its local subnet
D) X sends an ARP request packet with broadcast IP address in its local subnet
Ans.

18. Consider the following two statements.

S1: Destination MAC address of an ARP reply is a broadcast address.
S2: Destination MAC address of an ARP request is a broadcast address.

Which one of the following choices is correct?

A) Both S1 and S2 are true
B) S1 is true and S2 is false
C) S1 is false and S2 is true
D) Both S1 and S2 are false
Ans.

19. Consider the following clauses:

i. **Not inherently suitable for client authentication.**
ii. **Not a state sensitive protocol.**
iii. **Must be operated with more than one server.**
iv. **Suitable for structured message organization.**
v. **May need two ports on the serve side for proper operation.**

The option that has the maximum number of correct matches is

A) IMAP-i; FTP-ii; HTTP-iii; DNS-iv; POP3-v
B) FTP-i; POP3-ii; SMTP-iii; HTTP-iv; IMAP-v
C) POP3-i; SMTP-ii; DNS-iii; IMAP-iv; HTTP-v
D) SMTP-i; HTTP-ii; IMAP-iii; DNS-iv; FTP-v

Ans.

20. In a packet switching network, packets are routed from source to destination along a single path having two intermediate nodes. If the message size is 24 bytes and each packet contains a header of 3 bytes, then the optimum packet size is:

A) 4
B) 6
C) 7
D) 9

Ans.

21. Which one of the following statements is FALSE?

A) Packet switching leads to better utilization of bandwidth resources than circuit switching
B) Packet switching results in less variation in delay than circuit switching
C) Packet switching requires more per-packet processing than circuit switching
D) Packet switching can lead to reordering unlike in circuit switching

Ans.

22. Consider a network using the pure ALOHA medium access control protocol, where each frame is of length 1, 000 bits. The channel transmission rate is 1 Mbps (= 106 bits per second). The aggregate number of transmissions across all the nodes (including new frame transmissions and retransmitted frames due to collisions) is modelled as a Poisson process with a rate of 1, 000 frames per second. Throughput is defined as the average number of frames successfully transmitted per second. The throughput of the network (rounded to the nearest integer) is_____.

Ans.

23. For the IEEE 802.11 MAC protocol for wireless communication, which of the following statements is/are TRUE?

i. At least three non-overlapping channels are available for transmissions.
ii. The RTS-CTS mechanism is used for collision detection.
iii. Unicast frames are ACKed.

A) I, II, and III
B) I and III only
C) II and III only
D) II only

Ans.

24. The minimum frame size required for a CSMA/CD based computer network running at 1Gbps on a 200m cable with a link speed of 2 × 108m/sec is:

A) 125bytes
B) 250bytes
C) 500bytes
D) None of the above
Ans.

Practical-5

AIM: Understand and identify Layer-3 functionality.

Tools required:

1. Desktop Computer
2. Cisco Packet Tracer

Time distribution

Exercise-1	30 minutes
Exercise-2	30 minutes
Exercise-3	45 minutes
Questions and answer	15 minutes

Simulate different scenarios (Exercises-1 to 3) given below in Cisco packet tracker. Fill up respective tables, justify statements and write conclusion in your words.

Routing

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Types of routing

There are three types of routing as shown in figure 5.1.

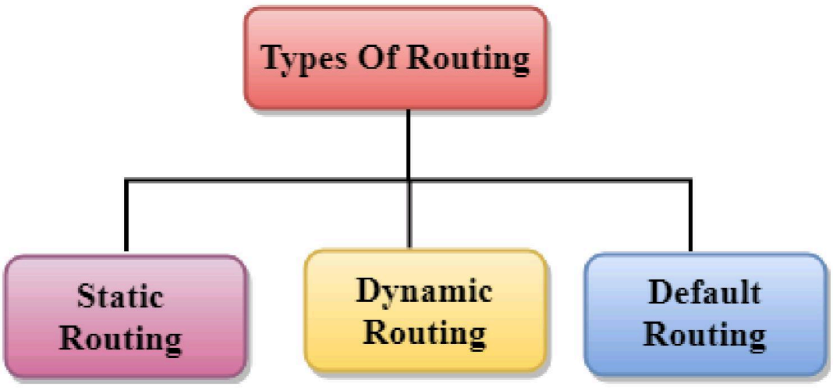


Figure 5.1

Static routing:

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.

Dynamic routing:

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.

Default routing:

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.

Routing Protocols

Routing protocols can be either an interior protocol or an exterior protocol. An interior protocol handles intradomain routing; an exterior protocol handles interdomain routing.

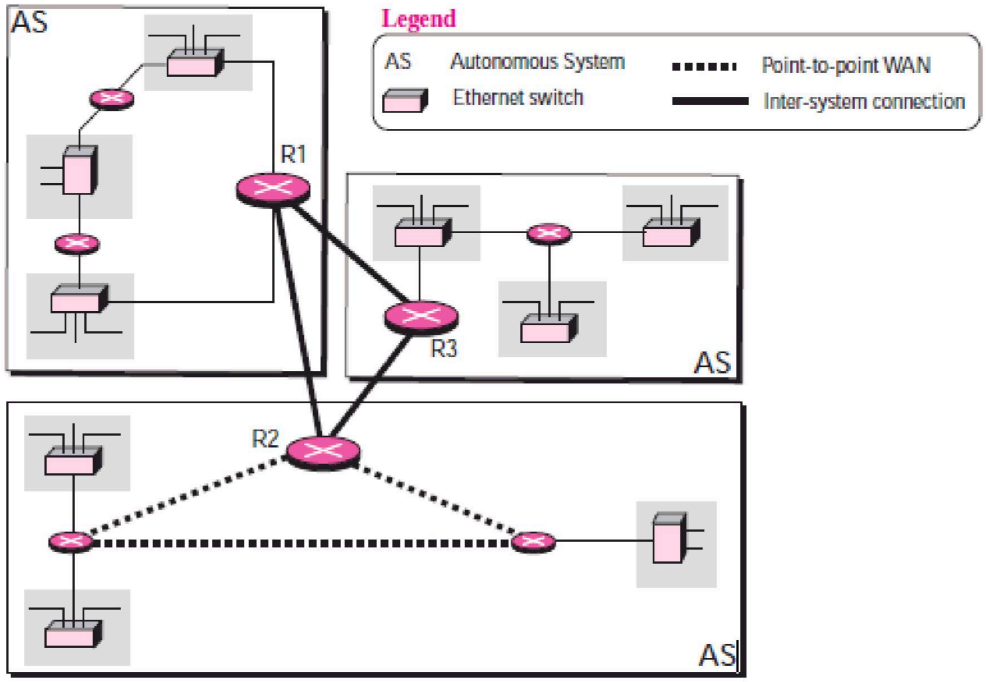


Figure 5.2 Intra domain and Inter domain routing protocol

Several intra-domain and inter-domain routing protocols are in use. We discuss two intra-domain routing protocols: distance vector and link state. We also introduce one inter-domain routing protocol: path vector.

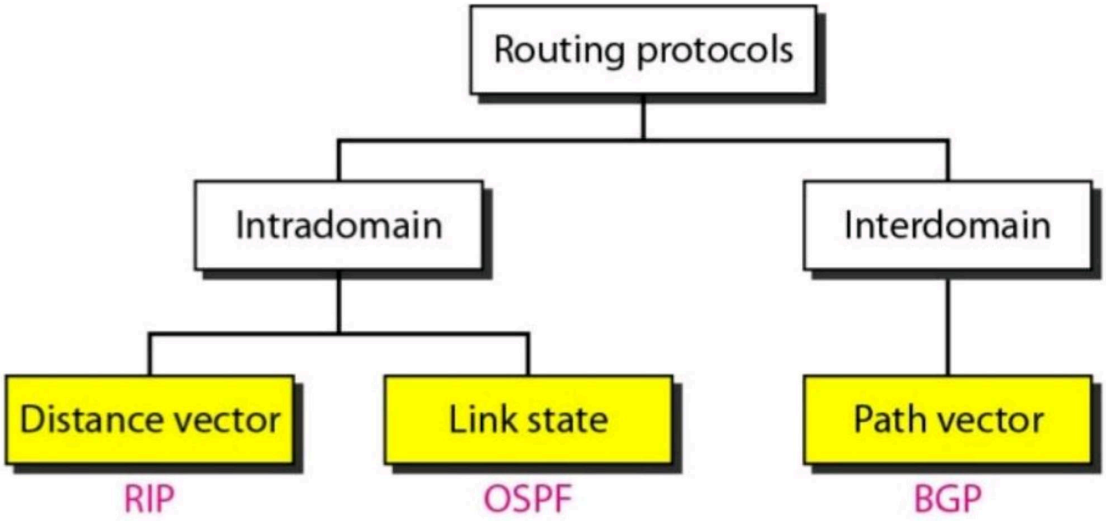


Figure 5.3 Routing Protocols

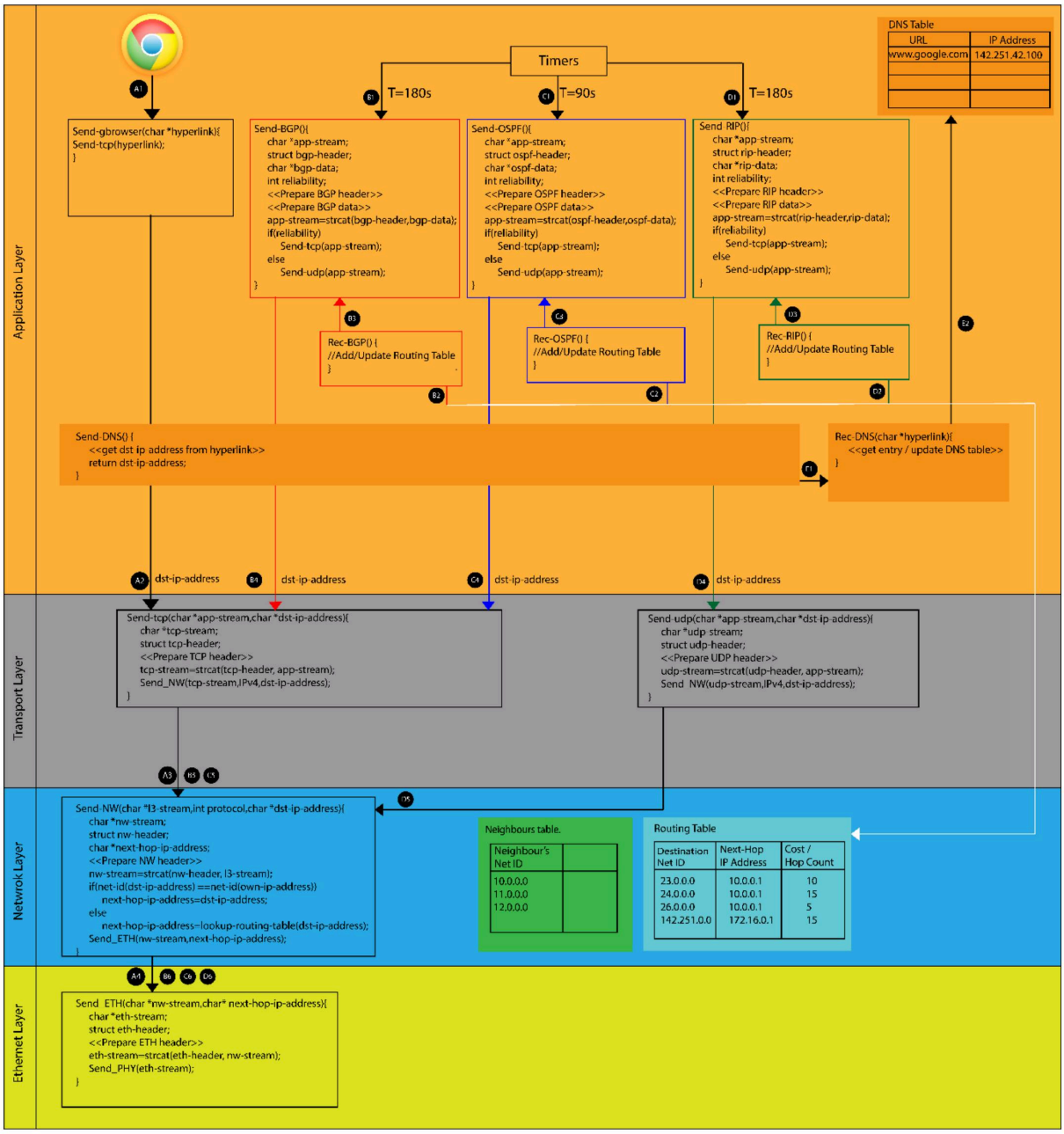
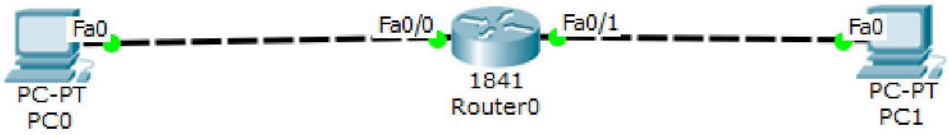


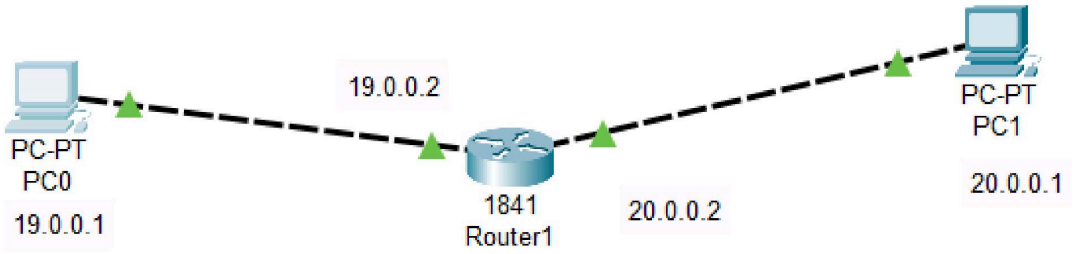
Figure 5.4 Demonstration of routing protocols in TCP/IP stack

1. How do DNS work?
   Ans. The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
2. What is the significance of the routing table?
   Ans. The routing table is a database that contains information about the paths between different networks. It is used by routers to determine how to forward packets to their destinations.
3. What is the next hop IP address?
   Ans. The next hop IP address is the IP address of the next router on the path to a destination network.
4. What is the significance of routing protocols?
   Ans. Routing protocols are an essential part of the internet infrastructure. They allow routers to efficiently route packets to their destination networks, which ensures that the internet is fast, reliable, and scalable.

Exercise-1



Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your knowledge.



Ping from PC0 to PC1 and vice versa and get the output here.

```
C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time=7ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 20.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms
```

Write down the ARP table of PC0 and PC1. Write down Routing table Router0.

ARP table entry of PC0

```
C:\>arp -a
  Internet Address      Physical Address      Type
  19.0.0.2              00e0.a384.7d01        dynamic
```

ARP table entry of PC1

```
C:\>arp -a
  Internet Address      Physical Address      Type
  20.0.0.2              00e0.a384.7d02        dynamic
```

Routing table of Router0:

Destination Network ID	Next Hop IP address	Hop Count along a path
10.0.0.0	--	0
11.0.0.0	--	0

Which are the following statements correct? Also justify each statement.

1. Is PC0 having Ethernet Card?
   Ans. Yes
   Justification: Because if we need to connect more ethernet we can insert it.

2. PC1 is having Ethernet Card.
   Ans. Yes
   Justification: Because if we need to connect more ethernet we can insert it.

3. Router0 is having two NIC card.
   Ans. Yes
   Justification: Because there are two fast ethernet ports.

4. Router 0 is having two Mac address
   Ans. Yes
   Justification: Because there are two fast ethernet ports.

5. Router0 is having TWO IP address
   Ans. Yes
   Justification: Because there are two fast ethernet ports.

6. MAC address pair on link 0(between PC0 and Router0) is different than MAC address pair in link 1(between Router0 and PC1) for message transfer.
   Ans. Yes
   Justification: Because MAC address of each device is unique.

7. Router0 is having switching table
   Ans. Yes
   Justification: To switch data within the network.

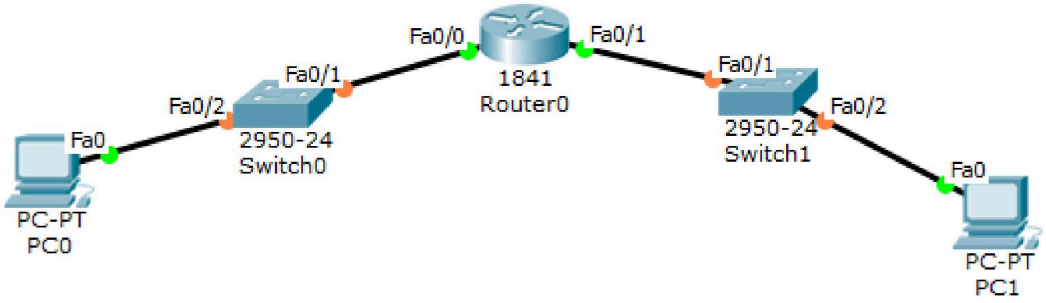
8. Speed of Link 0 is 10 Mbps.
   Ans. Yes
   Justification: There is more speed of link 1.

9. Speed of Link1 is 100 Mbps.
   Ans. Yes
   Justification: Because there is less speed of link0.

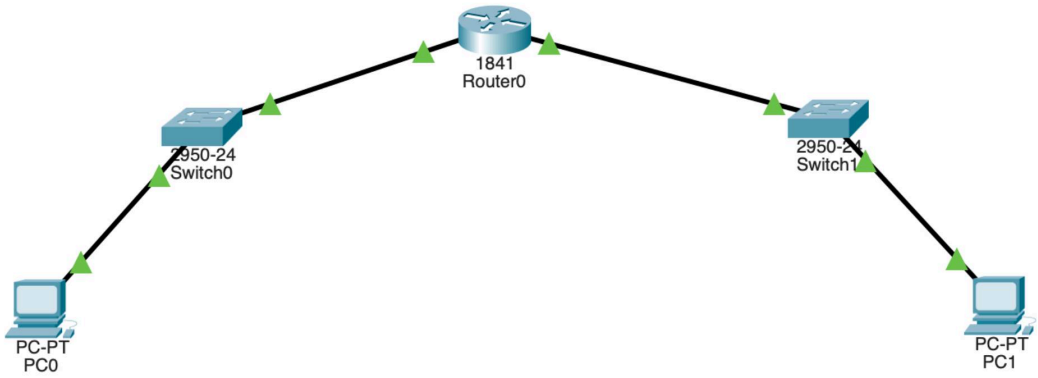
10. Router0 takes decision based on MAC address.
    Ans. Yes
    Justification: To reach to proper destination.

11. PC0 and PC1 can communicate because they are having same Ethernet cards i.e. Fa0.
    Ans. No
    Justification: Because they are in same network.
12. PC1 and Router0 cannot communicate as they are having different Ethernet cards.
    Ans. No.
    Justification: They cannot be ping to eachother.

Exercise-2



Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your knowledge.



Ping from PC0 to PC1 and vice versa and get the output here.

```
C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 20.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Write down ARP table of PC0 and PC1. Write down switch table of switches. Write down Routing table of routers.

ARP table entry of PC0

```
C:\>arp -a
  Internet Address      Physical Address      Type
  20.0.0.2              0005.5e8a.3802        dynamic
```

ARP table entry of PC1

```
C:\>arp -a
  Internet Address      Physical Address      Type
  20.0.0.2              0005.5e8a.3802        dynamic
```

Switch table entry of Switch0:

MAC Address	Ethernet port no
0090.2B0A.1168	1
0060.4766.0E01	2

Switch table entry of Switch1:

MAC Address	Ethernet port no
00D0.971E.02D8	1
0060.4766.0E01	2

Routing table of Router0:

```
Device Name: Router0
Device Model: 1841
Hostname: Router

Port              Link   VLAN   IP Address         IPv6 Address                          MAC Address
FastEthernet0/0   Up     --     19.0.0.2/8         <not set>                             0005.5E8A.3801
FastEthernet0/1   Up     --     20.0.0.2/8         <not set>                             0005.5E8A.3802
Vlan1             Down   1      <not set>          <not set>                             0050.0F59.D330

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0
```

Which are the following statements correct? Also justify each statement.

1. Switch0 contains MAC address of PC1 in their switching table.
   Ans. Yes
   Justification: Because they have to communicate.

2. Switch1 contains MAC address of PC1 in their switching table.
   Ans. Yes
   Justification: Because they have to communicate.

3. Any computer or device can be Router if it has two NIC cards.
   Ans. Yes
   Justification: Because it is connected to different device.

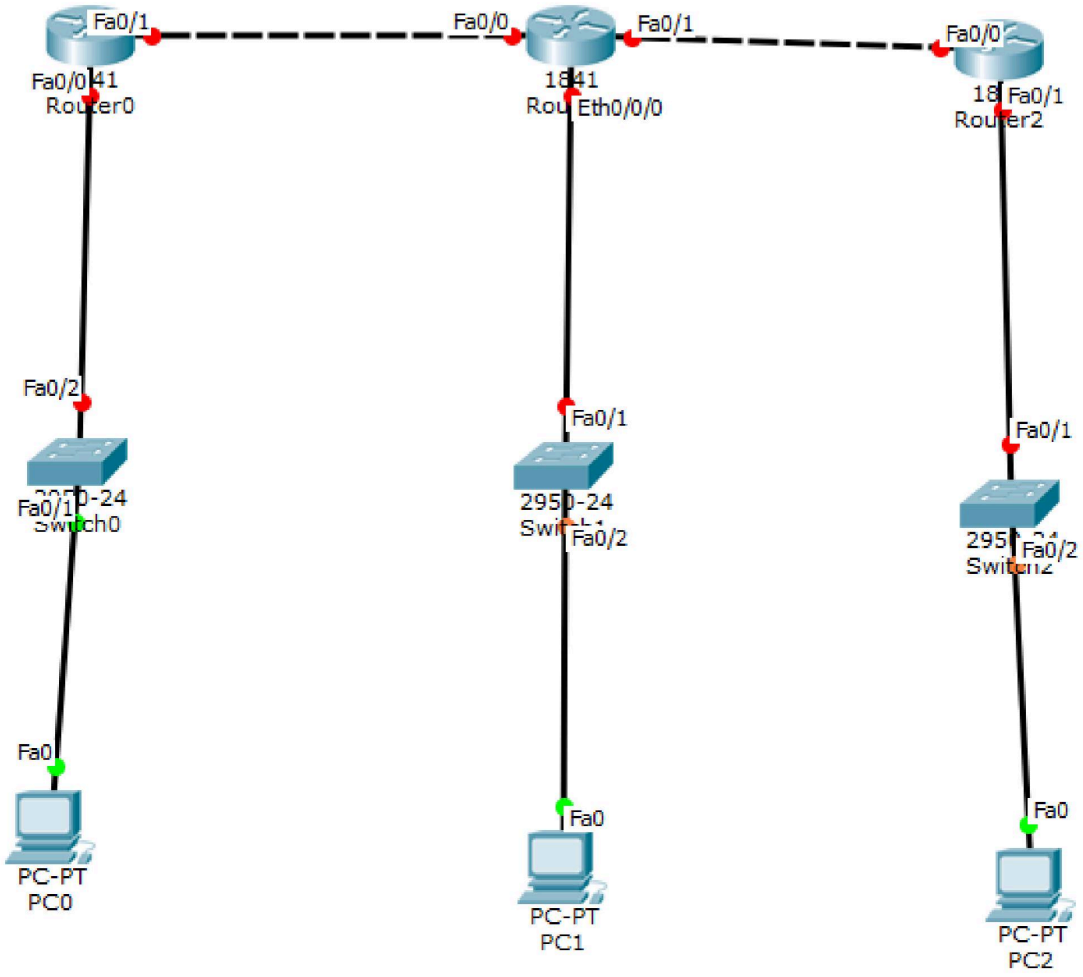
4. Switch0 and Switch1 may take decision based on IP address.

Ans. Yes
Justification: The nearest IP through them they send to it.

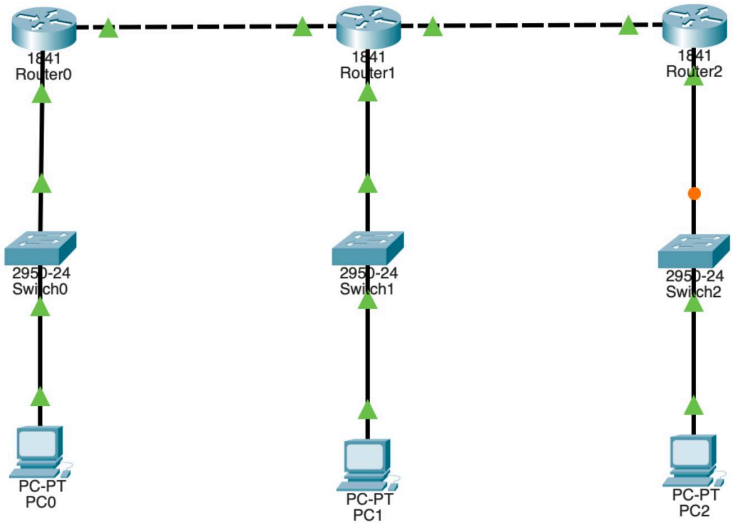
5. Router0 works at layer 3, while switches work at layer 2.
   Ans. Yes
   Justification: Router do data communication.
6. By default, Network ID of NIC cards are routing table entries.
   Ans. Yes
   Justification: By default, the routing table of a device will include a route for each network that the device is directly attached to.

7. MAC address pair on link 0(between PC0 and Router0) is different than MAC address pair in link 1(between Router0 and PC1) for message transfer.
   Ans. Yes
   Justification: Due to there MAC address and same network.

Exercise-3



Redraw above diagram which includes IP address and MAC address. Take IP address and MAC address as per your knowledge.



Ping all PCs respectively and get the output here.

```
C:\>ping 30.0.0.1

Pinging 30.0.0.1 with 32 bytes of data:

Reply from 37.0.0.2: Destination host unreachable.
Request timed out.
Reply from 37.0.0.2: Destination host unreachable.
Reply from 37.0.0.2: Destination host unreachable.

Ping statistics for 30.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 37.0.0.2: Destination host unreachable.
Reply from 37.0.0.2: Destination host unreachable.
Request timed out.
Reply from 37.0.0.2: Destination host unreachable.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Write down ARP table of PC0, PC1 and PC3 after successful ping. Write down switch table of switches. Write down Routing table of routers.

ARP table entry of PC0

```
C:\>arp -a
  Internet Address      Physical Address      Type
  37.0.0.2              0001.9634.7202        dynamic
```

ARP table entry of PC1

```
C:\>arp -a
  Internet Address      Physical Address      Type
  30.0.0.2              0001.42cc.281c        dynamic
```

ARP table entry of PC2

```
C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.2              0090.2bda.1d02        dynamic
```

Switch table entry of Switch0:

MAC Address	Ethernet port no
0009.7C73.ACC3	2
0001.9634.7202	1

Switch table entry of Switch1:

MAC Address	Ethernet port no

0007.EC59.7543	2
0001.42CC.281C	1

Routing table of Router0:

```
Device Name: Router0
Device Model: 1841
Hostname: Router

Port              Link   VLAN   IP Address         IPv6 Address                          MAC Address
FastEthernet0/0   Up     --     11.0.0.1/8         <not set>                             0001.9634.7201
FastEthernet0/1   Up     --     37.0.0.2/8         <not set>                             0001.9634.7202
Vlan1             Down   1      <not set>          <not set>                             0060.4716.22A9

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0
```

Routing table of Router1:

```
Device Name: Router1
Device Model: 1841
Hostname: Router

Port              Link   VLAN   IP Address         IPv6 Address                          MAC Address
FastEthernet0/0   Up     --     11.0.0.2/8         <not set>                             0007.EC07.5401
FastEthernet0/1   Up     --     37.0.0.3/8         <not set>                             0007.EC07.5402
Ethernet0/1/0     Up     --     30.0.0.2/8         <not set>                             0001.42CC.281C
Vlan1             Down   1      <not set>          <not set>                             00D0.BA6D.686C

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1
```

Routing table of Router2:

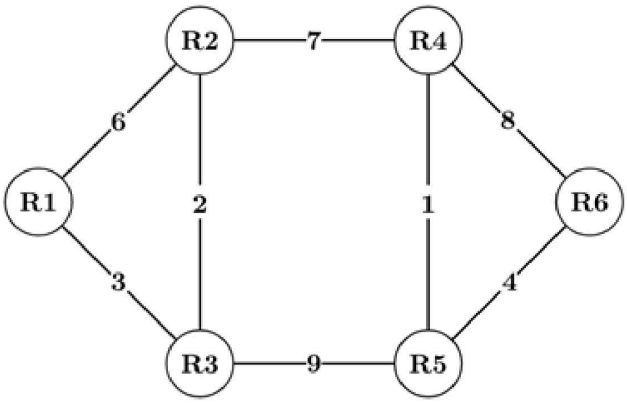
```
Device Name: Router2
Device Model: 1841
Hostname: Router

Port              Link   VLAN   IP Address         IPv6 Address                          MAC Address
FastEthernet0/0   Up     --     30.0.0.3/8         <not set>                             0090.2BDA.1D01
FastEthernet0/1   Up     --     10.0.0.2/8         <not set>                             0090.2BDA.1D02
Vlan1             Down   1      <not set>          <not set>                             000D.BD02.53E9

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router2
```

Conclusions (Inference):

1. We learned how to connect switch and routers together
2. We also learned how the network topology works.

GATE Questions:

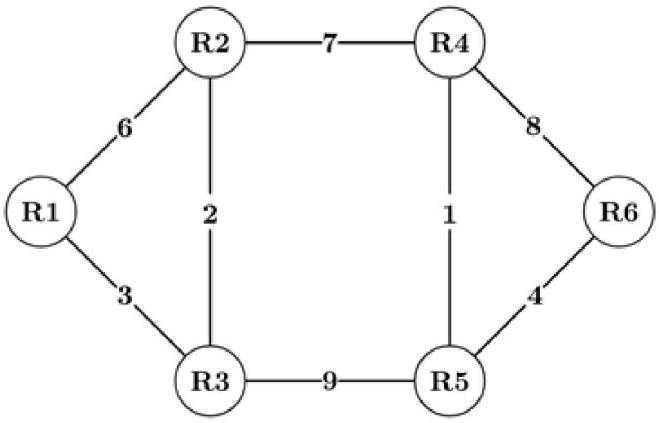
1. **Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram.**



All the routers use the distance vector-based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbor with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

A) 4
B) 3
C) 2
D) 1

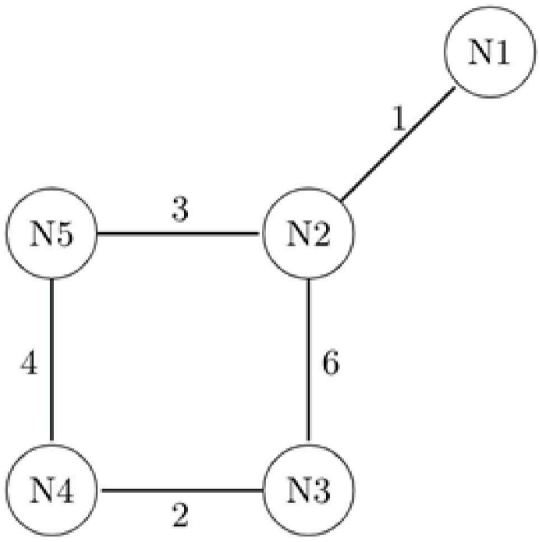
2. **Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram.**



Suppose the weights of all unused links are changed to 2 and the distance vector algorithm is used again until all routing tables stabilize. How many links will now remain unused?

A) 0
B) 1
C) 2
D) 3

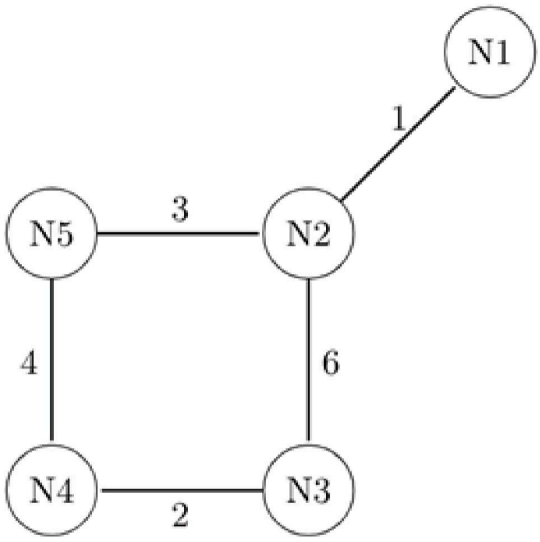
3. **Consider a network with five nodes, N1 to N5, as shown as below.**



The network uses a Distance Vector Routing protocol. Once the routes have been stabilized, the distance vectors at different nodes are as follows.
N1: (0, 1, 7, 8, 4)
N2: (1, 0, 6, 7, 3)
N3: (7, 6, 0, 2, 6)
N4: (8, 7, 2, 0, 4)
N5: (4, 3, 6, 4, 0)
Each distance vector is the distance of the best known path at that instance to nodes, N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbors. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors. The cost of link N2 – N3 reduces to 2 (in both directions). After the next round of updates, what will be the new distance vector at node, N3?

A) (3, 2, 0, 2, 5)
B) (3, 2, 0, 2, 6)
C) (7, 2, 0, 2, 5)
D) (7, 2, 0, 2, 6)

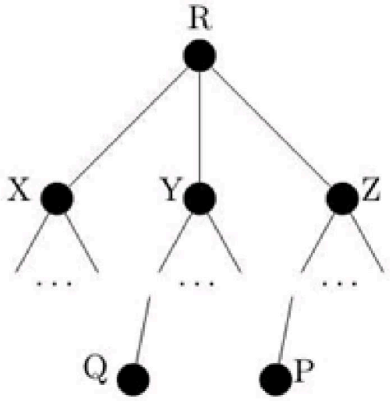
4. **Consider a network with five nodes, N1 to N5, as shown as below.**



The network uses a Distance Vector Routing protocol. Once the routes have been stabilized, the distance vectors at different nodes are as follows.
N1: (0, 1, 7, 8, 4)
N2: (1, 0, 6, 7, 3)
N3: (7, 6, 0, 2, 6)
N4: (8, 7, 2, 0,
N5: (4, 3, 6, 4, 0)
Each distance vector is the distance of the best known path at that instance to nodes, N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbors. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors. The cost of link N2 – N3 reduces to 2 (in both directions). After the next round of updates, the link N1 – N2 goes down. N2 will reflect this change immediately in its distance vector as cost, ∞. After the NEXT ROUND of update, what will be the cost to N1 in the distance vector of N3 ?

A) 3
B) 9
C) 10
D) ∞

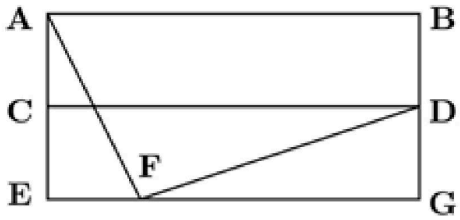
5. **Consider a computer network using the distance vector routing algorithm in its network layer. The partial topology of the network is shown below.**



The objective is to find the shortest-cost path from the router R to routers P and Q. Assume that R does not initially know the shortest routes to P and Q. Assume that R has three neighbouring routers denoted as X, Y and Z. During one iteration, R measures its distance to its neighbours X, Y , and Z as 3, 2 and 5, respectively. Router R gets routing vectors from its neighbours that indicate that the distance to router P from routers X, Y and Z are 7, 6 and 5, respectively. The routing vector also indicates that the distance to router Q from routers X, Y and Z are 4, 6 and 8 respectively. Which of the following statement(s) is/are correct with respect to the new routing table o R, after updation during this iteration?

A) The distance from R to P will be stored as 10
B) The distance from R to Q will be stored as 7
C) The next hop router for a packet from R to P is Y
D) The next hop router for a packet from R to Q is Z.

6. **For the network given in the figure below, the routing tables of the four nodes A, E, D and G are shown. Suppose that F has estimated its delay to its neighbors, A, E, D and G as 8, 10, 12 and 6 msecs respectively and updates its routing table using distance vector routing technique.**



Routing Table of A

A	0
B	40
C	14
D	17
E	21
F	9
G	24

Routing Table of D

A	20
B	8
C	30
D	0
E	14
F	7
G	22

Routing Table of E

A	24
B	27
C	7
D	20
E	0
F	11
G	22

Routing Table of G

A	21
B	24
C	22
D	19
E	22
F	10
G	0

A)

A	8
B	20
C	17
D	12
E	10
F	0
G	6

B)

A	21
B	8
C	7
D	19
E	14
F	0
G	22

C)

A	8
B	20
C	17
D	12
E	10
F	16
G	6

D)

A	8
B	8
C	7
D	12
E	10
F	0
G	6

7. Consider the following three statements about link state and distance vector routing protocols, for a large network with 500 network nodes and 4000 links.

[S1]: The computational overhead in link state protocols is higher than in distance vector protocols.
[S2]: A distance vector protocol (with split horizon) avoids persistent routing loops, but not a link state protocol.
[S3]: After a topology change, a link state protocol will converge faster than a distance vector protocol.
Which one of the following is correct about S1, S2, and S3?

A) S1, S2, and S3 are all true.
B) S1, S2, and S3 are all false.
C) S1 and S2 are true, but S3 is false.
D) S1 and S3 are true, but S2 is false.

Practical-6

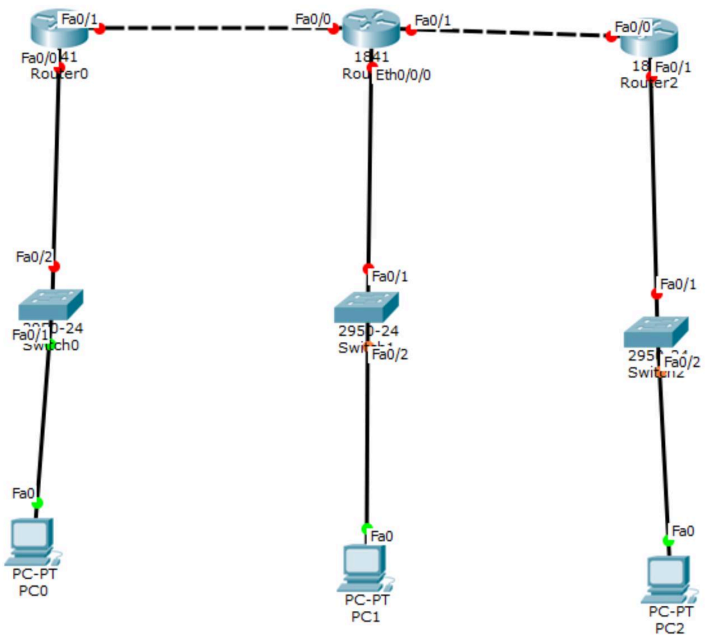
Date: 29-03-2024

AIM: Understand & identify Packet(L3) & frame(L2) content detail.

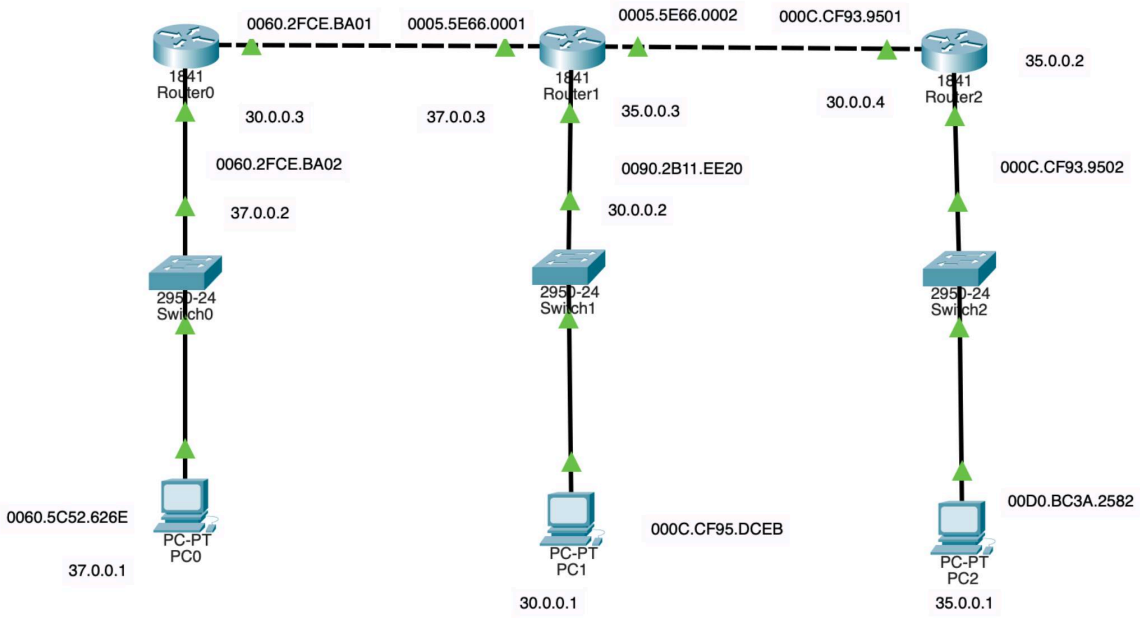
Tools required:
1. Desktop Computer
2. Cisco Packet Tracer

Note: While applying IP address, student need to allocate IP address as per his/her student ID. For Example, if student ID is 20ce005 then IP address allocation for first network should start with 5.0.0.0. For subsequent network, it should start with ID+1 i.e. 6.0.0.0, 7.0.0.0. and so on.

Submission: After writing answer into this word document, Student need to change name to his ID followed by practical number. Ex 20ce005_Pr1.docx. Upload on assignment segment.
Rubrics: Nicely drafted document with clarity in answers leads to full marks. Otherwise, submission carries proportional mark.
copy-past from cisco packet tracker is permitted.



Topology for the consideration



Steps:

1. Create topology in Realtime mode
2. Configure IP address
3. Configure Static Routing in Each routers
4. Ping from PC0 to rest other PCs and all interface of routers and fill success table
5. Go to Simulation mode
6. Prepare MAC and IP address Table.
7. Prepare ARP table for all PCs
8. Prepare Routing tables for Router0, Router1 and Router2
9. Prepare ARP tables for Router0, Router1 and Router2
10. Prepare MAC table of all switches
11. In simulation mode follow instructions as given in exercise and write answer of questions.

Destination machine	**Destination IP address**	**Command**	**Success/Fail**
FE0/0 of Router0	30.0.0.3	Ping 30.0.0.3	Success
FE0/1 of Router0	37.0.0.2	Ping 37.0.0.2	Success
FE0/0 of Router1	37.0.0.3	Ping 37.0.0.3	Success
FE0/1 of Router1	35.0.0.3	Ping 35.0.0.3	Success
FE0/0/0 of Router1	30.0.0.2	Ping 30.0.0.2	Success
PC1	30.0.0.1	Ping 30.0.0.1	Success
FE0/0 of Router2	30.0.0.4	Ping 30.0.0.4	Success
FE0/1 of Router2	35.0.0.2	Ping 35.0.0.2	Success

PC2	35.0.0.1	Ping 35.0.0.1	Success

Ping Success table

Ping from PC0 to PC2 and attach a snapshot for the same.

```
C:\>ping 35.0.0.1

Pinging 35.0.0.1 with 32 bytes of data:

Reply from 30.0.0.2: Destination host unreachable.
Reply from 30.0.0.2: Destination host unreachable.
Reply from 30.0.0.2: Destination host unreachable.
Request timed out.

Ping statistics for 35.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>arp -a
  Internet Address      Physical Address      Type
  30.0.0.2              0090.2b11.ee20        dynamic
```

Computer/Router Interface	**MAC address**	**IP address**
PC0	0060.5C52.626E	37.0.0.1
Router0 FE0/0	0060.2FCE.BA02	10.0.0.1
Router0 FE0/1	0060.2FCE.BA01	37.0.0.2
Router1 FE0/0	0005.5E66.0001	10.0.0.2
Router1 FE0/1	0005.5E66.0002	11.0.0.1
Router1 ETH0/0/0	0090.2B11.EE20	30.0.0.2
PC1	000C.CF95.DCEB	30.0.0.1
Router2 FE0/0	000C.CF93.9501	11.0.0.2
Router2 FE0/1	000C.CF93.9502	35.0.0.2
PC2	00D0.BC3A.2582	35.0.0.1

MAC and IP address Table

ARP Table for PC0

```
C:\>arp -a
  Internet Address      Physical Address      Type
  37.0.0.2              0060.2fce.ba02        dynamic
```

ARP Table for PC1

```
C:\>arp -a
  Internet Address      Physical Address      Type
  30.0.0.2              0090.2b11.ee20        dynamic
```

ARP Table for PC2

```
C:\>arp -a
  Internet Address      Physical Address      Type
  35.0.0.2              000c.cf93.9502        dynamic
```

Routing table for Router0

```
Device Name: Router0
Device Model: 1841
Hostname: Router

Port              Link   VLAN   IP Address        IPv6 Address                MAC Address
FastEthernet0/0   Up     --     10.0.0.1/8        <not set>                   0060.2FCE.BA01
FastEthernet0/1   Up     --     37.0.0.2/8        <not set>                   0060.2FCE.BA02
Vlan1             Down   1      <not set>         <not set>                   0060.47CD.1677

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0
```

Routing table for Router1

```
Device Name: Router1
Device Model: 1841
Hostname: Router

Port              Link   VLAN   IP Address        IPv6 Address                MAC Address
FastEthernet0/0   Up     --     10.0.0.2/8        <not set>                   0005.5E66.0001
FastEthernet0/1   Up     --     11.0.0.1/8        <not set>                   0005.5E66.0002
Ethernet0/1/0     Up     --     30.0.0.2/8        <not set>                   0090.2B11.EE20
Vlan1             Down   1      <not set>         <not set>                   000A.4103.AC1C

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1
```

Routing table for Router2

```
Device Name: Router2
Device Model: 1841
Hostname: Router

Port              Link   VLAN   IP Address        IPv6 Address                MAC Address
FastEthernet0/0   Up     --     11.0.0.2/8        <not set>                   000C.CF93.9501
FastEthernet0/1   Up     --     35.0.0.2/8        <not set>                   000C.CF93.9502
Vlan1             Down   1      <not set>         <not set>                   00D0.978C.47A5

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router2
```

IP Address	MAC Address	Interface
37.0.0.2	0060.2FCE.BA01	Dynamic
10.0.0.1	0060.2FCE.BA02	Dynamic

ARP Table for Router0

IP Address	MAC Address	Interface
10.0.0.2	0005.5E66.0001	Dynamic
11.0.0.1	0005.5E66.0002	Dynamic

ARP Table for Router1

IP Address	MAC Address	Interface
11.0.0.2	000C.CF93.9501	000C.CF93.9501
35.0.0.2	000C.CF93.9502	000C.CF93.9502

ARP Table for Router2

Switching table for Switch0

```
Device Name: Switch0
Device Model: 2950-24
Hostname: Switch

Port              Link   VLAN   IP Address        MAC Address
FastEthernet0/1   Up     --     --                0001.42EA.1A01
FastEthernet0/2   Up     --     --                0001.42EA.1A02
```

Switching table for Switch1

```
Device Name: Switch1
Device Model: 2950-24
Hostname: Switch

Port                Link   VLAN   IP Address          MAC Address
FastEthernet0/1     Up     --     --                  0000.0C5E.0201
FastEthernet0/2     Up     --     --                  0000.0C5E.0202
```

Switching table for Switch2

```
Device Name: Switch2
Device Model: 2950-24
Hostname: Switch

Port                Link   VLAN   IP Address          MAC Address
FastEthernet0/1     Up     --     --                  0005.5E13.9B01
FastEthernet0/2     Up     --     --                  0005.5E13.9B02
```

In simulation mode

Exercise-1: Ping from PC0 to FE0/0 of Router0

click on capture forward once so packet goes to switch, Inspect& write Inbound and Outbound PDU and fill following table

	In Bound	**Out Bound**
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0060.2FCE.BA02	0060.2FCE.BA02
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	10.0.0.1	10.0.0.1

Question: What decision will be taken by switch?

Answer: It will send packet to given MAC Address.

Exercise-2: Ping from PC0 to FE0/1 of Router0

Click on capture forward once so packet goes to switch, Inspect& write Inbound and Outbound PDU and fill following table

	In Bound	**Out Bound**
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0060.2FCE.BA01	0060.2FCE.BA01
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	37.0.0.2	37.0.0.2

Question: Is there any difference between table content of exercise-1 and 2? Why?

Answer: No, Because the destination is Same.

Exercise-3: Ping from PC0 to FE0/0 of Router1

Click on capture forward once so packet goes to switch, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	Out Bound
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0005.5E66.0001	0005.5E66.0001
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	10.0.0.2	10.0.0.2

Question: What decision will be taken by Router0?

Answer: Router0 will forward the msg.

Question: Is Inbound and outbound PDU detail remain same? If not why?

Answer: Yes.

Exercise-4: Ping form PC0 to PC1 (For even roll number of student PC0 to PC2)

Click on capture forward so packet goes to switch0, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	Out Bound
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	000C.CF95.DCEB	000C.CF95.DCEB
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	30.0.0.1	30.0.0.1

Click on capture forward so packet goes to Router0, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	Out Bound
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0060.2FCE.BA02	0060.2FCE.BA02
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	10.0.0.1	10.0.0.1

Click on capture forward so packet goes to Router1, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	Out Bound
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0005.5E66.0001	0005.5E66.0001
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	10.0.0.2	10.0.0.2

Click on capture forward so packet goes to switch1, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	Out Bound
Source MAC Address	0005.5E66.0001	0005.5E66.0001
Destination MAC address	0000.0C5E.0201	0000.0C5E.0201
Source IP Address	10.0.0.2	10.0.0.2
Destination IP address	30.0.0.1	30.0.0.1

Click on capture forward so packet goes to PC1, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	Out Bound
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0060.2FCE.BA01	0060.2FCE.BA01
Source IP Address	30.0.0.1	30.0.0.1

Destination IP address	30.0.0.2	30.0.0.2

Click on capture forward so packet goes to switch1, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	**Out Bound**
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0005.5E66.0001	0005.5E66.0001
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	10.0.0.2	10.0.0.2

Click on capture forward so packet goes to Router1, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	**Out Bound**
Source MAC Address	0005.5E66.0001	0005.5E66.0001
Destination MAC address	0000.0C5E.0201	0000.0C5E.0201
Source IP Address	10.0.0.2	10.0.0.2
Destination IP address	30.0.0.1	30.0.0.1

Click on capture forward so packet goes to router0, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	**Out Bound**
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0060.2FCE.BA02	0060.2FCE.BA02
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	10.0.0.1	10.0.0.1

Click on capture forward so packet goes to switch0, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	**Out Bound**
Source MAC Address	0060.5C52.626E	0060.5C52.626E
Destination MAC address	0005.5E66.0001	0005.5E66.0001
Source IP Address	37.0.0.1	37.0.0.1
Destination IP address	10.0.0.2	10.0.0.2

Click on capture forward so packet goes to PC0, Inspect & write Inbound and Outbound PDU and fill following table

	In Bound	**Out Bound**
Source MAC Address	0005.5E66.0001	0005.5E66.0001
Destination MAC address	0000.0C5E.0201	0000.0C5E.0201
Source IP Address	10.0.0.2	10.0.0.2
Destination IP address	30.0.0.1	30.0.0.1

Observe/inspect values of above tables and answer following questions.

Question: Is Source IP and Destination IP remains same for one way of data transmission?

Answer: No, it changes.

Justify: In reverse direction, source IP and destination IP address gets changed.

Answer: Yes it get change.

=Gate Questions :

1. **Which of the following functionality must be implemented by a transport protocol over and above the network protocol?**
   A) Recovery from packet losses
   B) Detection of duplicate packets
   C) Packet delivery in the correct order
   D) End to end connectivity
   Ans. **D) End to end connectivity**

2. **Choose the best matching between Group 1 and Group 2**

Group-1	Group-2
P. Data link layer	1.Ensures reliable transport of data over a physical point-to-point link
Q. Network layer	2.Encodes/decodes data for physical transmission
R. Transport layer	3.Allows end-to-end communication between two processes
	4. Routes data from one network node to the next

   A) P-1, Q-4, R-3
   B) P-2, Q-4, R-1
   C) P-2, Q-3, R-1
   D) P-1, Q-3, R-2
   Ans. **A) P-1, Q-4, R-3**

3. **Match the following:**

A. SMTP	1. Application Layer
B. BGP	2. Transport Layer
C. TCP	3. Data Link Layer
D. PPP	4. Network Layer
	5. Physical Layer

   A) A - 2, B - 1, C - 3, D - 5
   B) A - 1, B - 4, C - 2, D - 3
   C) A - 1, B - 4, C - 2, D - 5
   D) A - 2, B - 4, C - 1, D – 3
   Ans. **B) A-1, B-4, C-2, D-3**

4. **Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D.**
   A) Network layer – 4 times and Data link layer – 4 times
   B) Network layer – 4 times and Data link layer – 3 times
   C) Network layer – 4 times and Data link layer – 6 times
   D) Network layer – 2 times and Data link layer – 6 times
   Ans. **C) Network layer – 4 times and Data link layer – 6 times**

5. **In the following pairs of OSI protocol layer/sub-layer and its functionality, the INCORRECT pair is**
   A) Network layer and Routing
   B) Data Link Layer and Bit synchronization
   C) Transport layer and End-to-end process communication
   D) Medium Access Control sub-layer and Channel sharing
   Ans. **B) Data Link Layer and Bit synchoronization**

6. **Match the following:**

Field	Length in bits
(P).UDP Header's Port Number	I. 48
(Q).Ethernet MAC Address	II. 8
(R).IPv6 Next Header	III. 32
(S).TCP Header's Sequence Number	IV. 16

   A) P-III, Q-IV, R-II, S-I
   B) P-II, Q-I, R-IV, S-III
   C) P-IV, Q-I, R-II, S-III
   D) P-IV, Q-I, R-III, S-II
   Ans. **C) P-IV, Q-I, R-II, S-III**

7. **Which of the following is NOT true with respect to a transparent bridge and a router?**
   A) Both bridge and router selectively forward data packets
   B) A bridge uses IP addresses while a router uses MAC addresses
   C) A bridge builds up its routing table by inspecting incoming packets
   D) A router can connect between a LAN and a WAN
   Ans. **B) A bridge uses IP addresses while a router uses MAC address.**

8. **Which of the following is TRUE about the interior gateway routing protocols – Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)**
   A) RIP uses distance vector routing and OSPF uses link state routing
   B) OSPF uses distance vector routing and RIP uses link state routing
   C) Both RIP and OSPF use link state routing
   D) Both RIP and OSPF use distance vector routing
   Ans. **A) RIP uses distance vector routing and OSPF uses link state routing**

9. **An IP router implementing Classless Inter-domain Routing (CIDR) receives a packet with address 131.23.151.76 . The router's routing table has the following entries:**

Prefix	Outer Interface Identifier
131.16.0.0/12	3
131.28.0.0/14	5
131.19.0.0/16	2
131.22.0.0/15	1

   The identifier of the output interface on which this packet will be forwarded is _____.
   Ans. 1

10. Consider the following statements about the routing protocols. Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) in an IPv4 network.

I. RIP uses distance vector routing
II. RIP packets are sent using UDP
III. OSPF packets are sent using TCP
IV. OSPF operation is based on link-state routing

Which of the above statements are CORRECT?

A) I and IV only
B) I, II and III only
C) I, II and IV only
D) II, III and IV only

Ans. **C) I, II and IV only**

11. Consider the following statements about the functionality of an IP based router.

I. A router does not modify the IP packets during forwarding.
II. It is not necessary for a router to implement any routing protocol.
III. A router should reassemble IP fragments if the MTU of the outgoing link is larger than the size of the incoming IP packet.

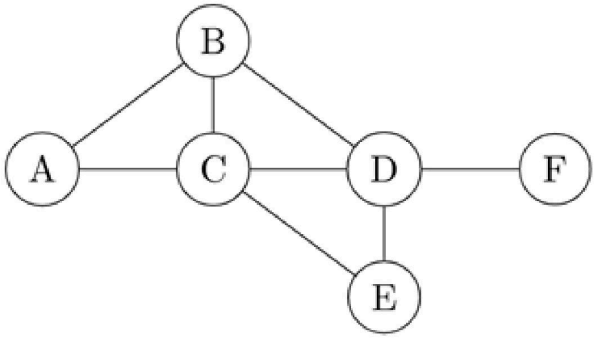
Which of the above statements is/are TRUE?

A) I and II only
B) I only
C) II and III only
D) II only

Ans. **II only**

12. Consider a simple graph with unit edge costs. Each node in the graph represents a router. Each node maintains a routing table indicating the next hop router to be used to relay a packet to its destination and the cost of the path to the destination through that router. Initially, the routing table is empty. The routing table is synchronously updated as follows. In each updated interval, three tasks are performed.

I. A node determines whether its neighbours in the graph are accessible. If so, it sets the tentative cost to each accessible neighbour as 1. Otherwise, the cost is set to ∞.
II. From each accessible neighbour, it gets the costs to relay to other nodes via that neighbour (as the next hop).
III. Each node updates its routing table based on the information received in the previous two steps by choosing the minimum cost.



For the graph given above, possible routing tables for various nodes after they have stabilized, are shown in the following options. Identify the correct table.

A.

A	-	-
B	B	1
C	C	1
D	B	3
E	C	3
F	C	4

Table for node A

B.

A	A	1
B	B	1
C	-	-
D	D	1
E	E	1
F	E	3

Table for node C

C.

A	A	1
B	-	-
C	C	1
D	D	1
E	C	2
F	D	2

Table for node B

D.

A	B	3
B	B	1
C	C	1
D	-	-
E	E	1
F	F	1

Table for node D

Ans. **A)**

13. A group of 15 routers is interconnected in a centralized complete binary tree with a router at each tree node. Router i communicates with router j by sending a message to the root of the tree. The root then sends the message back down to router j. The mean number of hops per message, assuming all possible router pairs are equally likely is

A) 3
B) 4.26
C) 4.53
D) 5.26

Ans. **C)5.26**

14. Two popular routing algorithms are Distance Vector(DV) and Link State (LS) routing. Which of the following are true?

(S1): Count to infinity is a problem only with DV and not LS routing
(S2): In LS, the shortest path algorithm is run only at one node
(S3): In DV, the shortest path algorithm is run only at one node
(S4): DV requires lesser number of network messages than LS

A) S1, S2 and S4 only
B) S1, S3 and S4 only
C) S2 and S3 only
D) S1 and S4 only

Ans. **D) S1 and S4 only**